UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Monika Lautar

Plačilni instrumenti

DIPLOMSKO DELO

UNIVERZITETNI PROGRAM RAČUNALNIŠTVA IN INFORMATIKE

Ljubljana, 2016

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Monika Lautar

Plačilni instrumenti

DIPLOMSKO DELO

UNIVERZITETNI PROGRAM RAČUNALNIŠTVA IN INFORMATIKE

MENTOR: doc. dr. Rok Rupnik

Ljubljana, 2016

[1] V dogovoru z mentorjem lahko kandidat diplomsko delo s pripadajočo izvorno kodo izda pod katero izmed alternativnih licenc, ki ponuja določen del pravic vsem: npr. *Creative Commons* **Error! Reference source not found.** in *GNU GPL* **Error! Reference source not found.**. Zgornje besedilo je opis licence, ki ga po potrebi lahko tudi prilagodite. Če se kandidat odloči, da diplomskega dela ne bo izdal pod omenjenimi licencami, je potrebno zgornje besedilo spremeniti v naslednje: »Rezultati diplomskega dela so intelektualna lastnina avtorja. Za objavljanje ali izkoriščanje rezultatov diplomskega dela je potrebno pisno soglasje avtorja, Fakultete za računalništvo in informatiko ter mentorja.« **V obeh primerih pa iz končnega besedila odstranite to opombo.**

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Diplomsko delo obravnava elektronske plačilne instrumente, ki se vpeljujejo v trgovska podjetja po svetu in v Sloveniji. Predstavljene so omejitve in prednosti prihajajočih načinov plačevanja. V sklopu diplomskega dela so opisane smernice, ki jih narekuje PCI Security Standard. Opisane so tehnologije, ki omogočajo sodobne plačilne instrumente. V zaključnem delu je opisana metodologija uvedbe spletne prodaje v trgovskem podjetju.

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisana Monika Lautar sem avtorica diplomskega dela z naslovom:

Plačilni instrumenti *(*angl. Payment instruments *)*

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelala samostojno pod mentorstvom doc. dr. Roka Rupnika
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 21.08.2016 Podpis avtorja:

Iskrena zahvala gospodu doc. dr. Roku Rupniku za strokovne nasvete pri pisanju naloge, ter karierne nasvete v času študija. Tudi poslovni kolegi imajo zelo dobro mnenje o njemu. Zahvala družini in posebej mojima fantoma za potrpljenje in razumevanje. Zahvala gre tudi podjetju Bankart d.o.o., ter sodelavcem v podjetju za pridobljeno strokovno znanje.

Kazalo

Seznam uporabljenih kratic

Kratica	Angleško	Slovensko
NFC	Near Field Communication	Visokofrekvenčna komunikacijska tehnologija kratkega dosega
SSL	Secure Sockets Layer	Kriptografski medmrežni protokol
EMV	Europay, MasterCard and Visa	Čip EMV
PIN	Personal Identification Number	Osebna identifikacijska številka
OTP	One Time Password	Enkratno geslo
POS	Point-of-sale	Prodajno mesto
EMU	European Monetary Union	Evropska monetarna unija
ECB	European Central Bank	Evropska centralna banka
PCI DSS	Payment Card Industry Data Security Standard	Standard varnosti podatkov kartičnega poslovanja
PCI SSC	PCI Security Standards Council	Svet PCI
PAN	Primary Account Number	PAN številka
CHD	Cardholder Data	Podatek o imetniku kartice
CVV	Card Verification Code	Varnostna koda na kartici
ASV	Approved Scanning Vendors	Verificirani izvajalci varnostnih pregledov
SAQ	Self-Assessment Questionnaire	Samoocenitveni vprašalnik PCI DSS

Povzetek

Naslov: Plačilni instrumenti

Diplomsko delo raziskuje področje plačilnih instrumentov in njihovo integracijo v trgovsko podjetje. V začetnem delu so podrobneje raziskane plačilne kartice kot najbolj zastopan plačilni instrument, ki je najbolj podvržen zlorabam ter prihajajočim spremembam. Za ustrezno teoretično podlago je izdelana razdelitev plačilnih karticah po različnih kriterijih. Eden od kriterijev je tehnologija izvedbe, ki nas skupaj z raziskavo evolucije plačilnih kartic, pripelje do zaključka, da se mediji za plačevanje dobrin in storitev nenehno spreminjajo. Potem, ko smo se skozi prvi, teoretični del seznanili s terminologijo plačilnih instrumentov in predvsem industrijo plačilnih kartic, ki jo usmerjajo in vodijo globalni ponudniki kartičnih shem, smo v osrednjem delu opisali standard PCI DSS, ki regulira poslovanje s plačilnimi karticami in vsem udeležencem nalaga skladnost s podanimi zahtevami. Ker standard PCI DSS za prodajna mesta - trgovce predvideva drugačno preverjanje skladnosti, ki je odvisna od števila letnih transakcij, ki jih trgovec opravi, je v diplomskem delu temu področju namenjeno ločeno poglavje. V zadnjem delu je za trgovinsko podjetje (trgovca) podana metodologija uvedbe spletne prodaje, ki svojim strankam poleg sodobnih tržnih poti omogoča sodobne plačilne instrumente, ki pa so kot je v osrednjem delu opisano, podvrženi strogim regulacijam predpisanih standardov.

Ključne besede: Plačilni instrumenti, plačilne kartice, plačilno mesto, bankomati, NFC, PCI DSS, PAN.

Abstract

Title: Payment instruments

The thesis is a survey of payment instruments and their integration to a trading company. Payment cards are explored in detail as the most performed payment instrument, and the most exposed to abuse and upcoming changes. For adequate theoretical basis, different criteria breakdown analysis is made. One of the criteria is implementation technology, which together with the study of payment cards` evolution, lead to the conclusion that the media for paying goods and services are constantly changing. In the central part of the thesis, PCI DSS standard is described, which regulates card payment transactions and demands compliance with specified requirements from all industry players. As PCI DSS standard for points-of-sale anticipates different compliance verification, depending on the annual number of transactions, performed by the trader-merchant, separate chapter is dedicated to that area. In the last part of thesis, methodology for implementation of online sales for trading company (merchant), which beside advanced commercial channels provides also modern payment instruments to its customers. However, payment instruments, as already described in the main part of the thesis, are a subject to highly restrictive standard regulations.

Keywords: Payment instruments, payment cards, point-of-sale, cash machines, NFC, PCI DSS, PAN

1. Uvod

Današnji potrošnik samoumevno jemlje enostavnost in minimalizem, ki mu jo omogoča plačilna kartica. Omogoča mu hiter način menjave svojih ali izposojenih denarnih sredstev za potešitev potreb ali želja.

Skozi zgodovino so se menjalna sredstva spreminjala in razvijala. Tako so recimo, na Kitajskem poznali menjavo dobrin za morske školjke. Zgodovina je kasneje pisala množico drugih najrazličnejših medijev, ki se jih je človek domislil. V zadnjem času smo priča umiku tudi tako imenovanega »plastičnega denarja«. Prihaja obdobje še večjega minimalizma in enostavnosti, kjer bo potrošnik vse imel na eni napravi oziroma na enem mediju.

Trenutno, sodobni načini plačevanja izpodrivajo uporabo gotovine. Imetniki bančnih računov, stranke ali drugače potrošniki, stremijo k minimalizmu. Poleg življenjsko nujnih pripomočkov (za veliko večino je to mobilna naprava), poleg sebe ne želijo drugih dodatkov. Ideja o združitvi vsega na en pripomoček (medij) nakazuje smer, h kateri se nagibajo izdajatelji vseh kartic (plačilnih, zdravstvenih, identifikacijskih, …).

Finančne inštitucije bodo v kratkem morale odgovoriti na vse večje povpraševanje potrošnikov po enostavnejšem in sodobnejšem načinu plačevanja, neposredno iz svojih bančnih računov na prodajnih mestih in bankomatih brez uporabe plačilnih kartic. Procesorski centri bodo morali bankam predstaviti rešitve, ki bodo omogočale prodajo takih produktov. Rešitve bodo morale v prvi vrsti zadostiti varnostnim standardom, ki jim že obstoječi plačilni instrumenti sledijo, hkrati pa bodo razširjene za nove tehnologije.

Trgovci, ki so prav tako vključeni v to zgodbo in brez katerih celotna zgodba ne bi obstajala, so se v glavnem že pričeli odzivati. Sodobne tržne poti, v prvi vrsti spletne prodaje, so že preskočile omejitve, ki so bile tradicionalno (fizično) prisotne v trgovinah - omejitev z delovnim časom, omejitve z lokacijo, omejitve z nacionalnimi valutami, dolgotrajnimi in dragimi postopki najemanja delovne sile, … .

S trendom umika gotovinskih plačil nastanejo prednosti tako za potrošnika, finančne inštitucije, ponudnike kartičnih shem, kot tudi za trgovce in države oz. nacionalna gospodarstva, saj se

zmanjšajo možnosti za nastanek sive ekonomije. Poleg tega, raziskave kažejo na sorazmernost uporabe plačilnih kartic z rastjo bruto domačega proizvoda.

S stalnim razvojem in prilagajanjem tehnologij zahtevam uporabnikov, denar sicer še vedno ostaja pojem plačilne sposobnosti, spreminja se le njegova oblika, dostopnost in transakcijska hitrost.

1.1. Motivacija

Skozi delovne naloge, ki jih opravljam vključujejo razvoj in vzdrževanje sistemov za obdelavo trenutno prisotnih plačilnih instrumentov, sem bila skeptična v ozadja in smernice, ki se vsiljujejo finančnem institucijam v Sloveniji. Vpeljava standardov skozi delovne naloge je zgolj implementacija dejanskih rešitev, oziroma omejitev ter nadzornih mehanizmov na informacijsko-komunikacijskih sistemih (omejitve dostopov, pregled kode, implementacija dnevniških zapisov z namenom revizijske sledi,…).

Standardi, ki se vpeljujejo so nedvomno nujni in poleg množice prednosti se porajajo tudi vprašanja, kot npr.; Ali zahteve po zaščiti teh podatkov niso preveč rigorozne in preveč usmerjena na znotraj (proti skrbnikom poslovnih sistemov in ne toliko proti zunanjim zlorabam).

Sodobni načini porabe denarnih sredstev potrošnikom dajejo vtis, da vse kar jim finančne inštitucije ponujajo, je v njihovo korist. Npr., da se potrošniku poenostavi plačevanje, da se zaščitijo njegovi podatki, da ima potrošnik večji pregled nad svojo porabo. Po drugi strani pa globalni ponudniki kartičnih shem dajejo vtis, da imajo z vpeljavo regulacij pri sodobnih plačilnih instrumentih, največ koristi trgovska podjetja. Skozi opise trenutno prisotnih plačilnih instrumentov, tehnologij, evolucije razvoja, predpisanih standardov, bomo poskušali odgovoriti, kaj se dogaja v ozadju in kdo vse ima koristi od tega, ko potrošnik porablja svoja denarna (razpoložljiva) sredstva.

Vsi akterji so morali že pri dosedanjem poslovanju slediti vrsti standardov, s katerimi so si zagotavljali dovoljenja za poslovanje. Standardi v prvi vrsti deklarirajo idejo zagotavljanja večje varnost podatkov imetnikov računov in njihovih sredstev, ter omejiti škodne primere za finančne inštitucije.

1.2. Cilji diplomskega dela

Strukturirana opredelitev plačilnih instrumentov, ki se uporabljajo in tržijo s strani finančnih akterjev, daje osnovo za nadaljnje raziskovanje tehnologij, ki omogočajo rešitve za mamljivo možnost plačevanja s mobilno napravo, neposredno iz bančnega računa. Da ta ideja ne bi bila preveč neresna in samo eksperimentalna, se je morajo vsi akterji v industriji plačilnih kartic lotiti s strogim upoštevanjem smernic in omejitev tako, kot se tega lotevajo z že vpeljanimi rešitvami. V drugem delu zato podajamo zahteve za zadostitev standardu.

Ker standard predpisuje omejitve za vse deležnike, se to nanaša tudi na trgovska podjetja ali trgovce. Cilj naloge je prikazati, kaj potrebuje trgovsko podjetje za umestitev svojega poslovanja v sodobno finančno procesiranje, če želi svojim strankam omogočiti hitro, enostavno in varno plačevanje blaga ali storitev preko spleta. Seznanitev s standardom za trgovca je predpogoj, če želi med obstoječe prodajne poti umestiti tudi prodajo preko spleta, ki pa ni smiselna brez uporabe elektronskih plačilnih instrumentov, med katere spadajo tudi plačilne kartice. Da bi se trgovinskemu podjetju ta integracija zdela obvladljiva, se v zaključnem delu predvideva umestitev metodologije za uvedbo spletne prodaje.

2. Plačilni instrumenti

Veliko vrst plačilnih instrumentov, ki so v Sloveniji na razpolago, pričajo o tem, kako so se banke in ostale finančne institucije pripravljene prilagoditi zahtevam komitentov, če želijo obdržati ali pridobiti konkurenčno prednost. Med vsemi plačilnim instrumenti kaže največji porast uporaba plačilnih kartic oz. plastičnega denarja ter različne izvedbe le-tega.

Opredelitev pojma »plačilni instrument«

Zakon o plačilnih storitvah in sistemih (Uradni list RS, št. 58/09, 34/10, 9/11, 32/12 in 81/15)
15. člen (plačilni instrument in pridobivanje plačilnih instrumentov)
(1) Plačilni instrument pomeni vsako napravo ali niz postopkov oziroma oboje, ki so dogovorjeni med posameznim uporabnikom in njegovim ponudnikom plačilnih storitev, in je vezan le na tega uporabnika z namenom, da ga uporabi za odreditev plačilnega naloga [1].

Glede na obliko prenosa v plačilnem prometu se denarna sredstva prenašajo bodisi gotovinsko bodisi v negotovinskih oblikah prenosa. Negotovinske oblike prenosa pridobivajo vedno večjo vlogo za razliko od gotovinskih oblik poravnavanja denarnih obveznostih, ki so v upadanju.

2.1. Plačilni instrumenti, kot jih opredeljuje Evropska komisija

Evropski plačilni trg Evropska komisija opredeljuje [2]:

1. **Osnovni plačilni instrumenti** (kreditni prenosi in neposredne bremenitve). Za ta dva plačilna instrumenta obstajajo vseevropske plačilne sheme, in sicer SEPA (SCT) pravilnik kreditnih prenosov in pravilnik neposrednih bremenitev SEPA (SDD), ki ju je za plačila v evrih razvil Evropski svet za plačila.

2. **Plačilne kartice**. Evropska komisija jih uvršča med elektronske plačilne instrumente. Trenutno so plačilne kartice najpogosteje uporabljen elektronski plačilni instrument.

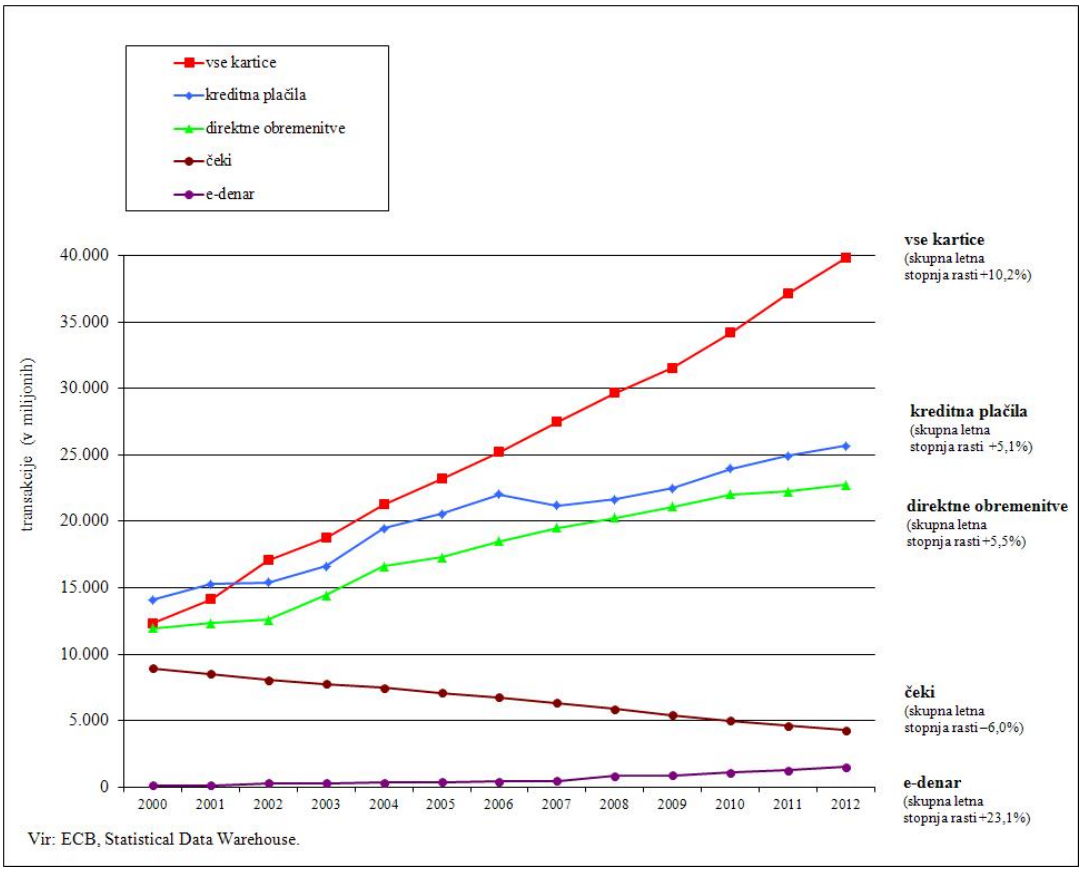
3. **Plačila prek spleta (e-plačila).** V to kategorijo uvrščajo:

   3.1. spletne transakcije s plačilno kartico na daljavo,

   3.2. transakcije prek spletnega bančništva s kreditnimi ali neposrednimi bremenitvami,

   3.3. transakcije preko ponudnikov e-plačil, pri katerih je potrošnik odprl posamezen račun

   E-plačila pridobivajo pomembnejšo vlogo vzporedno s porastom in prodajo v spletnih trgovinah. Evropska komisija ugotavlja, da je v tej kategoriji še veliko neizkoriščenega potenciala za rast. Ena od glavnih ovir za bodočo rast transakcij v spletnih trgovinah so ravno plačila.



Slika 1: Uporaba glavnih plačilnih instrumentov v EU (2000-2013) [44]

4. **Mobilna plačila (m-plačila)** so plačila, za katera se podatki in navodila z zvezi s plačilom odpošljejo, prenesejo ali potrdijo preko mobilnega telefona ali naprave. To kategorijo razdelijo na:

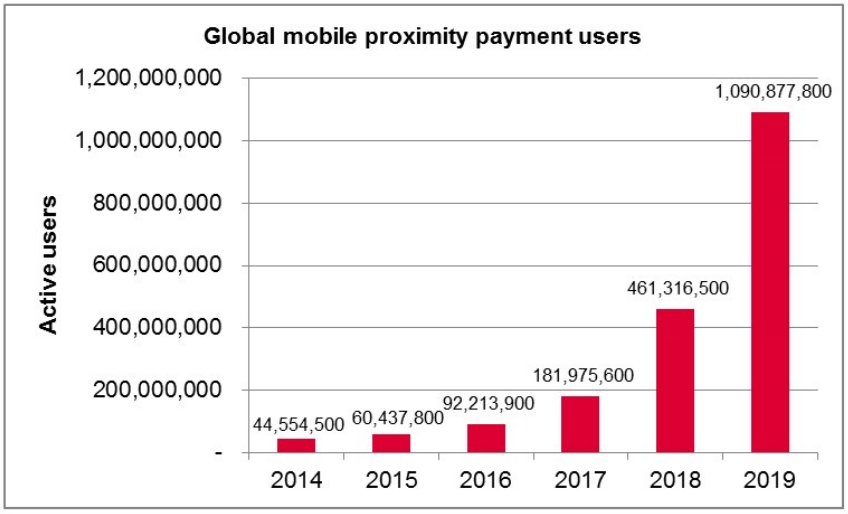
   4.1. M-plačila na daljavo. Večina m-plačil na daljavo trenutno temelji na shemah kartičnih plačil. Druge rešitve, ki temeljijo na kreditnih prenosih ali neposrednih bremenitvah, so tehnično izvedljive ter enako varne, učinkovite in konkurenčne, vendar se zdi da se težko prebijajo na trg.

   4.2. Brezstična plačila na splošno potekajo neposredno na prodajnih mestih. Z uporabo visokofrekvenčne komunikacijske tehnologije kratkega dosega (NFC), kot trenutno vodilne tehnologije na področju brezstičnih plačil, je za plačila potrebno imeti posebno opremljene mobilne naprave, ki jih je mogoče prepoznati v bližini čitalniškega modula na prodajnem mestu (npr., trgovina, javni prevoz, …) ali bankomatu.

   Plačila prek mobilnih telefonov so trenutno najhitreje rastoča med vsemi plačilnimi metodami. K temu razvoju je prispeval hiter porast pametnih telefonov z možnostjo namestitve sodobnih plačilnih aplikacij.

V Evropi je še veliko potenciala za povečanje zastopanosti mobilnih plačil. Eden od ključnih razlogov je velika razdrobljenost trga, tako na strani mobilnih operaterjev, ponudnikov plačilnih storitev, kot tudi proizvajalcev mobilnih telefonov. Obstaja pa vzorčen primer dobre prakse o skupnem poslovnem modelu, kot ga EMU pozna za kreditna plačila, debetna plačila in kartično poslovanje (v Sloveniji še ni vpeljan), ki spadajo v skupino **SEPA shem**.

Nekatere raziskave kažejo, da mobilna brezstična plačila zavzemajo najmanjši delež plačil, hkrati pa so najhitrejše rastoči segment (Slika 2).



Slika 2: Napoved rasti števila uporabnikov mobilnih brezstičnih plačil [20]

2.2. Plačilne kartice

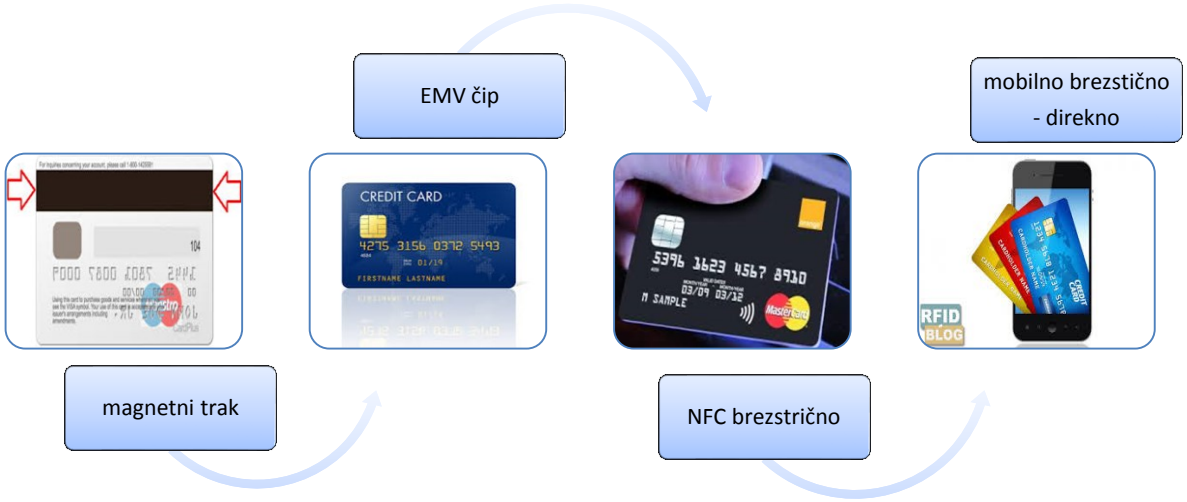
Plačilni instrument so tudi plačilne kartice, ki jih imetniki lahko uporabljajo za dvig gotovine na bankomatu ali za plačilo na POS terminalu. Plačilna kartica ima vgrajen elektronski nosilec podatkov, ki uporabniku omogoča plačevanje na elektronskem terminalu, v breme sredstev na njegovem transakcijskem računu oziroma v breme računa izdajatelja plačilne kartice in sicer ob pogoju, da uporabnik pozna enolično identifikacijsko kodo, oziroma se s podpisom izkaže kot upravičeni imetnik plačilne kartice. Razvrščamo jih po različnih kriterijih. Predvsem s pravnega in finančnega vidika sta pomembna predvsem način poravnave in kriterij izdajatelja plačilne kartice.[33]

Trendi mobilnih plačil nakazujejo smer, ko bo vse, kar je na plastični plačilni kartici, preneseno na mobilno napravo. Brezstične kartice so že dodobra zastopane v slovenskem prostoru. Na ta način bi lahko sklepali, da gre samo za vmesno stopnjo pred vpeljavo mobilnih brezstičnih plačil.

2.2.1. Evolucija

Pojava prvih plačilnih kartic sega v leto 1950. Od takrat se njihovo število nenehno povečuje. Pri tem prednjači Amerika pred Evropo. V Sloveniji so se začele uporabljati v šestdesetih letih prejšnjega stoletja in so doživele večji razmah, ko so pričeli domači izdajatelji in ponudniki kartic aktivno delovati.

Plačilne kartice so se skozi čas razvijale predvsem na področju povečanja varnosti oz. zmanjšanja možnosti za zlorabe.



Slika 3. Evolucija plačilnih kartic glede na tehnologijo izvedbe
Vir: Lasten

2.2.2. Delitev plačilnih kartic

Plačilne kartice so danes nepogrešljivi dodatek vsakega potrošnika. V veliki množici različnih kartic jih je težko razčleniti v skupine. Jasno je, da so plačilne kartice samo del množice vseh izvedb kartic, ki obstajajo. Razvoj kartic je v prvi vrsti usmerjen v zmanjšanje možnosti zlorab. Drugi vidik je hitrost oz. poenostavitev izvedbe transakcije. Kazalci kažejo, da s poenostavljanjem izvedbe transakcije, imetniki kartic zapravijo več. Od tega imajo največ koristi trgovci, banke, izdajatelji kartic, procesni centri in nenazadnje tudi nacionalna gospodarstva.
Večja pozornost v prihodnje bo namenjena brezstičnim karticam, ki v zadnjem času pridobivajo na veljavi, in ki jih banke množično uvrščajo v svoje kartične sheme. Banke se poleg tega odločajo še za ohlapnejša stališča preverjanja istovetnosti imetnika (neobvezen PIN za manjše zneske).

Delitev glede na funkcijo, ki jo opravljajo:

- **Predplačniške kartice**, ki jih vnaprej kupimo in jih lahko zavržemo. Preden jih uporabimo nanje naložimo dobroimetje. So enake oblike kot kreditne ali debetne kartice. Te kartice imajo svoje prednosti. V primeru izgube ali zlorabe je imetnik lahko oškodovan samo za del sredstev, ki jih ima na svojem osebnem računu.

- **Debetne kartice** so vezane na osebni račun odprt pri eni izmed poslovnih bank. Omogočajo plačevanje in dvigovanje gotovine v okviru sredstev, ki so na razpolago na osebnem računu imetnika kartice. Višina enkratnega dviga, dnevnega limita, višina transakcijskega zneska je odvisna od bančnega produkta, za katerega se je imetnik kartice odločil in ga vzel pri banki izdajateljici.

- **Kreditne kartice** so kartice z odloženim plačilom, pri katerih nas izdajatelj kartice bremeni samo enkrat na mesec, do plačila pa nas izdajatelj kreditira.

- **Posojilne kartice**, ki nam omogočajo obročno poravnavo dolga. Primer: Banka za uporabo posojilne kartice odobri okvirno posojilo, na primer 1.000 evrov. S kartico si lahko kadarkoli izposodite poljuben znesek, dokler vsota vseh zneskov ne doseže še dovoljene največje vrednosti (1.000 evrov). Višina deleža posojila, ki ga boste odplačali vsak mesec, se določi v pogodbi. Če se bo ob koncu meseca na vaši kartici

nabralo 1.000 evrov dolga in je s pogodbo določeno, da vsak mesec odplačate po deset odstotkov posojila, ostane še 900 evrov dolga. Za ta znesek vam bo banka zaračunala obresti in jih prištela k dolgu. Če bi bile obresti na koncu meseca 10 evrov, bi bilo tako vaše novo stanje na kartičnem računu 910 evrov. Enak postopek se ponovi vsak mesec [4].

Delitev glede na izdajatelja kartice

- **Bančne kartice:** Izdajajo jih banke samostojno ali na podlagi pogodbe z velikimi izdajatelji, kot so: American Express, MasterCard, Visa, Diners Club. Domače bančne kartice so tudi Activa in Maestro.

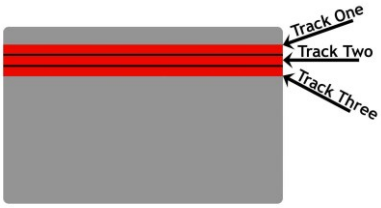
- **Podjetniške kartice:** Izdajajo jih podjetja. V Sloveniji so to v glavnem trgovska podjetja (Mercator, Petrol, …). S temi karticami podjetja kupcem lahko ponujajo ugodnosti in točke zvestobe.

- **Partnerske kartice**: Izdajajo jih podjetja v sodelovanju z bankami. To so lahko kartice ugodnosti, (Enka, Merkur, Delo, …).

- **Licenčne kartice**: V tem primeru ima pravico do izdaje ena domača banka. Vse ostale banke imajo licenco za izdajanje in so odvisne od banke izdajateljice oz. »acquirer bank«. Med take kartice spadajo npr., MasterCard, Visa, Diners, AmericanExpress.

Delitev glede na tehnologijo izdelave

Magnetna steza: Kartice z magnetno stezo imajo v magnetnem zapisu shranjene podatke, ki so potrebni za izvedbo transakcije – podatki o imetniku, podatki o izdajatelju, podatki o možnostih limita, možnostih dvigovanja gotovine ali plačevanja. Po uvedbi čip kartice ali pametne kartice, tovrstna izvedba plačilnih kartic izgublja na pomenu in uporabi . Slabost te izvedbe je razmeroma enostavno kopiranje zapisa iz magnetne steze, kar predstavlja velik problem zagotavljanja varnosti. Na ameriškem tržišču so še vedno zastopane v veliki meri [5].

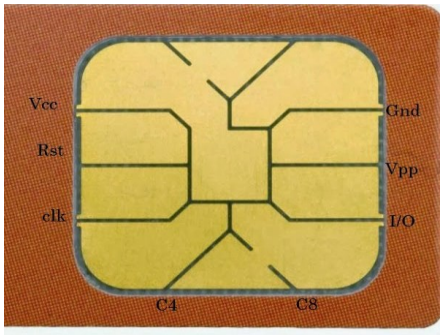


Slika 4: Magnetna steza [21]

Pametne kartice ali mikroprocesorske kartice. Te kartice imajo namesto magnetne steze integriran mikroprocesor na čipu. Omogočajo dinamično obdelovanje podatkov in njihovo shranjevanje. Dinamičnost in večja kapaciteta shranjenih podatkov omogoča večjo varnost in hkrati manjšo možnost zlorabe. Imetnik svojo identiteto potrjuje z osebno identifikacijsko številko (PIN). V svetu se uporablja še naziv kartica z integriranim vezjem (ang. ICC - Integrated Circuit Card).

Očitne prednost mikroprocesorskih kartic so naslednje:

- Zelo težko je klonirati tovrstne kartice. Še posebej to velja za varne kriptografske parametre katere vsebujejo, v primeru da ni umaknjena zaščita.
- Skozi postopek procesiranja transakcije, mikročip aktivno sodeluje v preprečevanju zlorab na sami lokaciji nakupa. Nastopa v vlogi izdajatelja v okviru katere se lahko preprečijo zlorabe.
- Naprednejše je tudi ugotavljanje ponarejenih kartic, ker se uporablja metoda avtentikacije z dinamičnem mehanizmom. Omogoča tudi večjo varnost imetniku kartice pri off-line uporabi (npr., v primeru ko ni internetne povezave), oziroma verifikaciji in pri vnosu PIN-a [7].



Slika 5: Mikroprocesor na kartici [22]

Na sliki (Slika 5) so podrobneje navedeni deli mikročipa, ki je v osnovi majhen računalnik. V grobem je čip razdeljen na tri dele in sicer na spomin, mikroprocesor ter vhodno/izhodno enoto. Vcc predstavlja napajanje, GND označuje ozemljitev, RST – ponastavljanje (reset), Vpp - napetost za programiranje, clk – predstavlja uro ter oznake C4, C8 rezervirano [6].

Taka kartica ima dve značilnosti, ki onemogočata zlorabo in ponarejanje. Ena od teh je spomin, ki se ga ne da spreminjati in se ohrani tudi po prekinitvi napajanja. Ta spomin lahko vsebuje tudi informacije, ki so bile zapisane po tem, ko je bila kartica izdana, in lahko zabeleži vsako transakcijo. S tem prepreči lastniku, da bi prekoračil svoj limit. Druga značilnost pa je, da procesorski center kontrolira vse interakcije med različnimi zunanjimi enotami, ki berejo kartico in pišejo nanjo, in spominom pametne kartice. Ta je oblikovan tako, da so določeni deli spomina fizično in logično dostopni le izdajatelju kartice [7].

Pametne kartice niso omejene samo na bančno panogo. V širšem pomenu jih lahko delimo na kartice z finančnimi aplikacijami in na kartice z nefinančnimi aplikacijami (telekomunikacije, zdravstvo, šolstvo in vojska).

Brezstične ali brezkontaktne kartice

Trenutno v Sloveniji skoraj vse banke v okviru svojih kartičnih shem ponujajo brezstične plačilne kartice. Poleg prednosti, ki jih imajo mikročip kartice, so te nadgrajene še za enoto, ki omogoča brezkontaktno komunikacijo plačilne kartice in čitalca (POS terminal ali bankomat). Dodatna enota je mikroantena ali NFC (Near Field Communication) čip, ki je integriran v kartico in, ki navzven ni viden. Taka kartica je opremljena s posebno oznako. Tehnologiji in standarda, ki sta v uporabi za tovrstno izvedbo, sta RFID (ang. Radio-Frequency Identification) ali NFC protokola.

Tehnologija z NFC protokolom uporablja enostavno navezo čipa in elektromagnetnega navitja, ki v osnovi niti ne potrebuje napajanja. Elektrone za posredovanje informacij mu da magnetno polje, ki ga ustvari aktivni oddajnik oziroma bralnik. Tok je dovolj močan, da zmore naprava s šibko jakostjo oddati nekaj malega podatkov [8].

Slika 6: oznaka na brezstični kartici

Brezstičen način plačevanja je še posebej primeren za tista prodajna mesta, kjer je hitrost transakcije ključnega pomena. Brezstična kartica nima neposrednega kontakta in je ni potrebno nikamor vložiti. Dovolj je da k posebnemu brezstičnemu terminalu približate kartico. Podatke in energijo prenaša na več načinov, kot so induktivni, optični »Capacitive Coupling, Microvawe Coupling,…idr.«, in glede na to deluje na razdalji 1mm ali pa nekaj metrov (kot npr. , ko na avtocesti čitalec zazna brezkontaktno kartico v avtu, ki vozi do 100km na uro). Brezkontaktna kartica ima številne prednosti pred kontaktno kartico, saj je zanesljivejša, njena življenjska doba je daljša ter omogoča hitrejšo in enostavnejšo uporabo. Bralna enota nima reže, tak da je manj možnosti za vandalizem (npr. lepilo, žvečilni gumi v reži) [7].

2.2.3. Glavni akterji

Na tržišču s plačilnimi karticami nastopajo ponudniki shem plačilnih kartic, izdajatelji, pridobitelji, procesni centri ter ponudniki kartične infrastrukture, ki omogočajo izvajanje plačil s plačilnimi karticami.

Omenili smo že, da imajo s samo izvedbo transakcije koristi tako banke, veliki izdajatelji kartic, kot tudi procesni centri z zaračunavanjem provizij. Ne smemo pozabiti, da negotovinsko plačevanje kot tàko omogoča omejevanje sive ekonomije, od katerega imajo posredno korist nacionalna gospodarstva z zaračunavanjem davkov.

Na sliki (Slika 7) je prikazano zaračunavanje različnih provizij (ang. Fees) od vsake izvedene transakcije na POS terminalu.

Slika 7: Pobiranje provizij od vsake izvedene transakcije [23]

V svetovnem merilu prevladujejo štirje večji ponudniki plačilnih shem: Visa, MasterCard, Diners Club in American Expres. Vsak od teh ponuja plačilne kartice, ki jih za njih izdajajo banke v različnih plačilnih shemah. V tem pogledu taki banki pravimo banka izdajateljica (ang. Issuing Bank). Imetnik kartice (ang. Cardholder) uporablja plačilno kartico za plačevanje blaga in storitev. Trgovci oz. ponudniki blaga ali storitev (ang. Merchant) ali drugače lastniki prodajnih mest, plačujejo provizije za sprejem plačilnih kartic. Te provizije znašajo približno 1 do 4 odstotka zneska vsake transakcije.

2.2.3.1. Globalni ponudniki shem plačilnih kartic

Omenjeno je bilo že, da so najbolj znana podjetja za kreditne kartice Visa, MasterCard, American Express, Diners. V eno skupino spadata Visa in MasterCard, v drugo pa American Express in Diners. Panoga plačilnih kartic (ang. PCI - Payment Card Industry) obsega vse entitete, ki hranijo, procesirajo in distribuirajo podatke o imetnikih kartic (ang. Cardholder Data). Najpogosteje so to podatki o imetnikih debetnih in kreditnih kartic. Svét, ki so ga leta 2004 ustanovila podjetja American Express, Discover Financial Services, JCB International, MasterCard Worldwide in Visa Inc. z imenom PCI SSC (PCI Security Standards Council), je zadolžen za širjenje zavedanja o boljši zaščiti podatkov imetnikov plačilnih kartic. Visoki standardi o varovanju osebnih podatkov na ravni bank so se tako še

nadgradili s varnostnimi programi članov svéta. Skupek teh varnostnih zahtev je združen v standardu PCI DSS (Payment Card Industry Data Security Standard), ki pogojuje poslovanje vsem entitetam v prometu s plačilnimi karticami (trgovci, procesni centri, lastniki prodajnih mest, banke). Trenutna verzija standarda je 3.2,ki je bila objavljena aprila 2016.

2.2.3.2. Izdajatelji plačilnih kartic

Poleg globalnih ponudnikov shem plačilnih kartic, obstajajo tudi domači izdajatelji in ponudniki kartic. V Sloveniji so se plačilne kartice pričele uporabljati v 60. Letih prejšnjega stoletja. Omenjeno je bilo že, da plačilne kartice ločimo tudi glede na izdajatelje. Lokalni izdajatelji (banke in družbe) izdajajo licenčne kartice (Visa, MasterCard, Diners, American Express) in imajo svoje bankomate ter POS terminale, na katerih opravljajo transakcije vsi imetniki kartic (Cardholderji), tudi tujci (imetniki plačilnih kartic, katerih izdajateljice so tuje finančne institucije).

Izdajatelji ali ponudniki plačilnih storitev pripadajo posamični kartični shemi. Izdajatelji so banke in druge finančne organizacije kot tudi podjetja, ki ponujajo storitve plačevanja blaga in storitev ter dvig gotovine za svoje kupce. Nazor nad uporabo plačilnih kartic v Sloveniji izvaja Banka Slovenije. Domači izdajatelj plačilne kartice je pravna oseba s sedežem v Sloveniji, tuji izdajatelj plačilne kartice ima sedež izven Slovenije [9].

2.2.3.3. Procesni centri

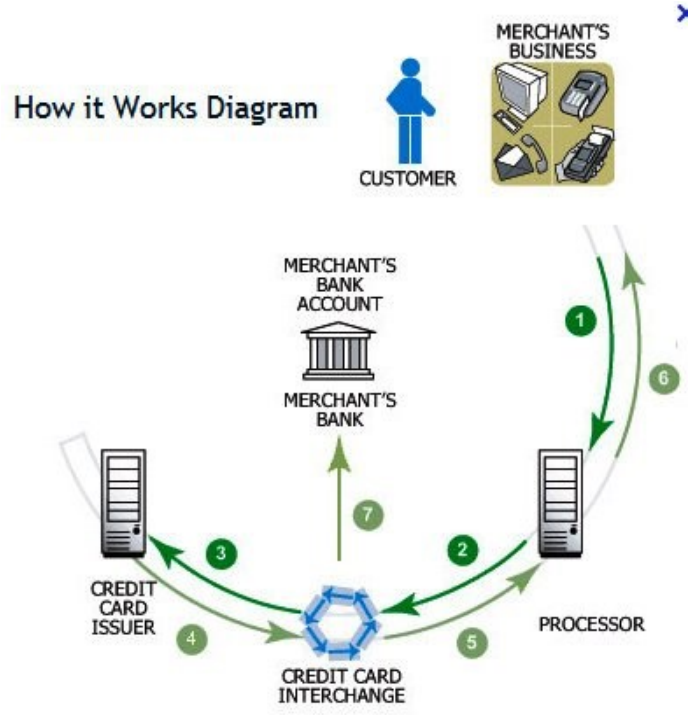
Procesni centri ali procesorji so podjetja , ki upravljajo s transakcijami iz različnih kanalov za debetne, kreditne in ostale plačilne kartice za banke trgovcev in banke, ki so izdajateljice kartic. Plačilno transakcijo je potrebno v zelo kratkem času obdelati, kar pomeni, da je potrebno preveriti podrobnosti o imetniku kartice pri banki izdajateljici, preveriti množico parametrov proti zlorabami kartice, preveriti dovoljeno stanje ter izvesti transakcijo. Enkrat ko procesni center dobi potrdilo, da je kartica veljavna, se potrditev pošlje na vhod banke trgovca, ki lahko pošlje pozitiven odgovor za plačilno transakcijo. Če do potrditve ne pride, procesni center pošlje obvestilo banki trgovca, ki transakcijo zavrne.

2.2.4. Interesi glavnih akterjev na trgu plačil s karticami

Interesi med glavnimi akterji so različni. Kot prvo, so tukaj medbančne provizije ali medbančna nadomestila, ki jih pridobitelji običajno prenesejo na izdajatelje, ki pripadajo eni od shem, ter jih pridobitelji zaračunajo trgovcem za vsako kartično transakcijo . Trgovci nato te kartične stroške tako kot vse druge stroške vključijo v splošne cene blaga in storitev. Kot drugo, so tudi interesi kartičnih shem, da prepričajo čim več ponudnikov plačilnih storitev (izdajatelji), da izdajajo njihove kartice, zaradi česa so medbančne provizije na trgu običajno višje.

Na prvi pogled bi se dalo sklepati, da imajo z uvedbo standardov (PCI DSS) največ koristi imetniki računov, ker so njihova sredstva in podatki bolj zaščiteni, ali da imajo koristi finančne inštitucije. Ozadje standarda kaže, da so predpise in smernice predpisali ravno globalni ponudniki kartičnih shem, ki nalagajo vsem entitetam pogoje za poslovanje.

2.2.5. Procesiranje plačilnih kartic

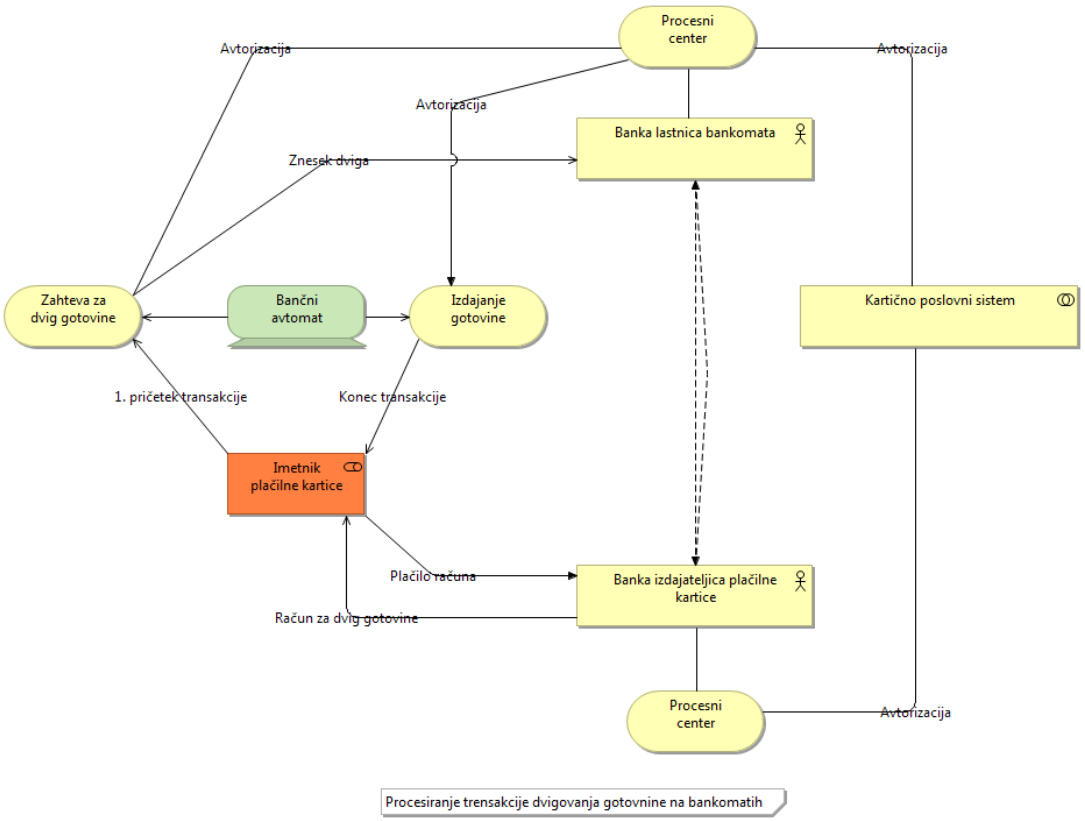


Slika 8. Procesiranje kartičnega poslovanja [24]

Ker se tržišča plačilnih kartic razlikujejo med državami in ker so procesne prakse zelo različne, je v nadaljevanju podana predstavitev poteka transakcije na bankomatu in POS terminalu, ki so trenutno v uporabi na slovenskem tržišču plačilnih kartic.

2.2.5.1. Procesiranje transakcije na bankomatu v Sloveniji

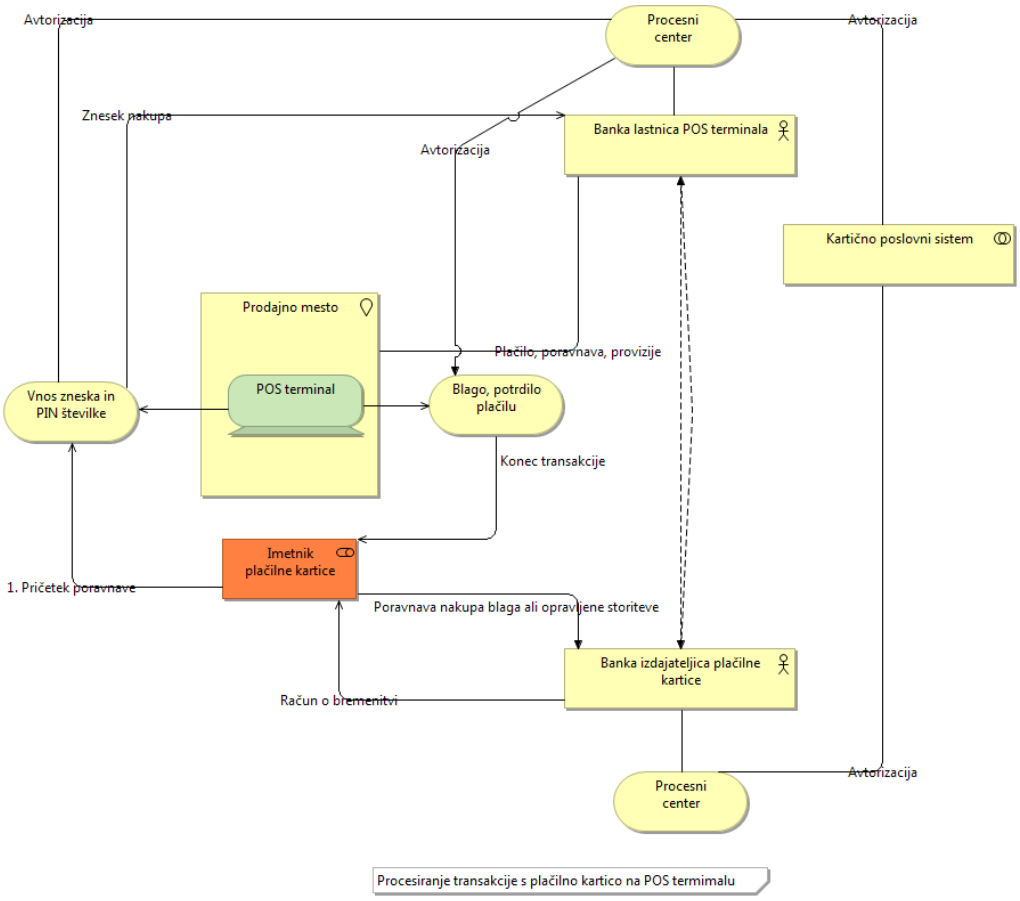
Transakcija dviga gotovinskih sredstev na bankomatu se prične z vstavitvijo plačilne kartice v režo bankomata. Od imetnika plačilne kartice nato bankomat zahteva vnos PIN številke. Imetnik potem izbere storitev - dvig gotovine in vnese še željen znesek. Potem se zahteva za transakcijo pošlje banki lastnici bankomata oz. bolj natančno, njenemu procesnem centru, ki jo obdela. Obračuna se promet in medbančna provizija, izdajatelj plačilne kartice pa bremeni račun imetnika plačilne kartice za izplačan znesek.



Slika 8: Procesiranje na bankomatih v Sloveniji
Vir: Lasten

2.2.5.2. Procesiranje transakcije na POS terminalu v Sloveniji

Plačilna transakcija na POS terminalu se prične z zahtevo kupca oziroma imetnika kartice, da poravna kupljeno blago ali opravljeno storitev s svojo plačilno kartico. Trgovec vnese znesek transakcije. Imetnik kartice ali trgovec prisloni (pri kartici z NFC tehnologijo), povleče (kartica z magnetnim trakom) ali vtakne (kartica z pametnim čipom) v POS terminal – odvisno od tehnologije izvedbe kartice. Trgovec s potrditvijo sproži preverjanje plačilne sposobnosti imetnika kartice pri banki izdajateljici plačilne kartice, ki preko procesnega centra poda odgovor banki trgovca prodajnega mesta. S tem se zaključi potrditveni (avtorizacijski) del transakcije. Po tem, ko banka izdajateljica sporoči, da je izvedba transakcije možna, imetnik kartice (odvisno od višine zneska), vnese PIN številko. Po uspešnem preverjanju PIN številke potrdilo o izvedeni transakciji prejmeta trgovec in kopijo lastnik plačilne kartice. Iz POS terminalov se ob zaključku dneva pošlje seznam vseh transakcij banki lastnici prodajnega mesta. Procesni center posreduje transakcije bankam izdajateljicam oziroma globalnim ponudnikom kartičnih shem, če gre za mednarodno plačilno kartico. Banka izdajateljica poravna v sklopu domačih ali tujih dogovorov terjatve banki lastnici prodajnega mesta. Tudi banka lastnica prodajnega mesta poravna obveznosti po pogodbenih obveznostih trgovcu za vse sprejete kartice, ne glede na banko izdajateljico. Odvisno od tipa plačilne kartice, se imetnika kartice bremeni avtomatsko oziroma pri kreditnih karticah lahko samo enkrat mesečno.



Slika 10: Procesiranje transakcij s plačilno kartico na POS terminalu
Vir: Lasten

2.3. Mobilni plačilni instrumenti – direktni

Poleg prej omenjenih možnostih plačevanja se v zadnjem času pojavljajo sodobnejši načini plačevanja. Finančne institucije bodo morale v zelo kratkem času odgovoriti na vse večje povpraševanje imetnikov bančnih računov po možnostih mobilnega plačevanja za opravljene storitve ali nakup blaga. Mobilno plačevanje je relativno nova in še neuveljavljena praksa finančnih transakcij, pri katerih se porajajo predvsem vprašanja, povezana z varnostjo.

Interes kupcev za tovrstno izboljšavo plačevanja je velik, saj fizična prisotnost plačilne kartice ni potrebna. Prisotnost mobilne naprave prekaša vse ostale pripomočke, dokumente in ostalo

opremo, ki jo ima posameznik ob sebi, pa naj bo v vlogi potrošnika, plačnika, uporabnika ali stranke.

Evolucijsko gledano, so brezstične kartice vmesna stopnja pri izboljšavi načinov plačevanja. Brezstično sicer trenutno lahko plačujemo na nekaterih prodajnih mestih. Bankomati slovenskih bank še ne omogočajo brezstično dvigovanje gotovine. Trenutno je v Sloveniji že dobro vpeljana brezstična kartica, ki ima integriran brezžični računalniški čip. Tak čip prenaša podatke o transakciji iz prodajnega mesta.

Vpeljava takega načina plačevanja, predstavlja dodatne investicije v varnost, v nadgradnjo plačilnih mest (POS terminali), ter zamenjavo ali nadgradnjo bankomatov ter nadgradnjo poslovnih procesov.

Že prej smo opisali tehnologije, ki omogočajo direktne mobilne načine plačevanja. Med vsemi tehnologijami se največkrat omenja NFC tehnologija. Napovedana možnost plačevanja z mobilnimi napravami ter z uporabo NFC tehnologije, brez nadgradnje ali zamenjave bankomatov nima dobre prihodnosti. Komitenti bank, ki pričakujejo umik plačilnih kartic in prestavitev njihove funkcionalnosti na mobilne naprave, želijo celovito uporabnost ne glede na to ali plačujejo na POS terminalu ali dvigujejo gotovino na bančnem avtomatu.

Naslednji logični korak v evoluciji plačevanja je mobilno plačevanje, ki prav tako spada v skupino elektronskih plačil kot plačilne kartice in, ki za izvedbo transakcije potrebuje enake elemente kot plačilna kartica, le tehnologija izvedbe je drugačna. Na ta način lahko vidimo, tako kot je v uvodu zapisano, da se je skozi zgodovino plačevanja dobrin spreminjal in razvijal medij, tako, da je sedaj nastopilo obdobje izvedbe plačevanja z mobilno napravo.

Po definiciji je mobilna naprava tista, ki ima prilagojen operacijski sistem kot so iOS, Android, BlackBerry OS, Windows mobile, in je mobilna (mobilni telefoni, tablični računalniki, ipd.). V to kategorijo lahko uvrstimo tudi vse naprave, ki se lahko prenašajo in se z njihovo pomočjo dostopa do interneta brez fizične povezave - brezžično (torej tudi prenosniki, prenosne igralne konzole, industrijski čitalci, ipd.) [15].

V poglavju (2.2.2. Delitev plačilnih kartic), kjer smo opredeljevali plačilne kartice glede na tehnologijo izvedbe, smo omenili tudi izvedbo z rešitvijo NFC tehnologije. Mobilna naprava s katere želimo izvesti brezstično plačevanje ali dvigovanje denarja na bankomatu mora podpirati to tehnologijo. V tem primeru govorimo o direktnem mobilnem plačevanju, ki ga moramo ločiti od mobilnega plačevanja kot so Moneta, Hal mBills, Urbana in druge rešitve, ki so prisotne v slovenskem plačilnem prostoru in denarna sredstva porabljajo iz nekega vmesnega računa, ki je del rešitve. Pogoj, da potrošnik izvaja transakcije s temi mobilnimi rešitvami je nakazilo

denarja na te račune. Take posredne rešitve izpostavljajo nekatere ključne vidike. Eden od teh je, da z nakazili sredstev na vmesni račun ne ogrožamo vseh denarnih sredstev in svojega bančnega računa. Drugi vidik je, da je potrebna dodatna aktivnost preliva denarnih sredstev na vmesni račun. Tretji vidik oz. vprašanje je, ali so vedno vsa sredstva na vmesnem računu porabljena, ali mogoče ostanejo neporabljena. Možni vzroki so lahko: prenehanja uporabe ali izguba medija.

Plačevanje z uporabo NFC tehnologije preko mobilne naprave se izvaja z bremenitvijo plačilnega računa , ki je izdan s strani finančne institucije. Pri tem so aplikacija in podatki o računu varno shranjeni na mobilni napravi. Telefon uporablja NFC tehnologijo za komuniciranje z brezstičnim POS terminalom trgovca na podoben način, kot se danes uporabljajo brezstične plačilne kartice in naprave. Procesi izvedbe transakcij so enaki procesom, ko stranka plačuje s klasično brezstično plačilno kartico oz. s kartico z magnetnim trakom.

Varnost

Vsaka aplikacija, ki je na kakršenkoli način vključena v proces obdelave, prenašanja ali shranjevanja plačilnih transakcij ali podatkov o njej, mora zadostiti visokim varnostnim zahtevam. Na primer, informacije o plačilnem računu in plačilni transakciji morajo biti strogo zaščitene, medtem, ko tiste, ki se nanašajo na samo prodajo izdelkov oziroma storitev, nudijo oziroma zahtevajo nižjo stopnjo varnosti, oziroma so celo brez.

NFC plačila s kreditnimi ali debetnimi plačilnimi aplikacijami so varna. Osebni podatki, ki vključujejo finančne informacije kot sta številka računa in datum veljavnosti računa, so shranjene na varnem mestu v NFC telefonu, ki se običajno imenuje **varnostni element.**

Varnostni element

Medtem, ko vse NFC aplikacije ne zahtevajo varnosti, pa tiste, ki vključujejo finančne transakcije, določene mobilne trženjske aplikacije ali druge aplikacije, ki morajo zaščititi uporabnikovo kredibilnost, zahtevajo na telefonu **varnostni element** z namenom varnega shranjevanja aplikacij in/ali kredibilnosti in zagotavljajo varno izvajanje aplikacij.

Varnostni element (varnostni spomin in izvedbeno okolje) je dinamično okolje v katerem so lahko aplikativna koda in aplikativni podatki varno shranjeni, se z njimi upravlja in v katerem se aplikacija varno izvaja. Element se nahaja v visoko varovanem šifrirnem čipu (običajno čip

pametne kartice). Element ima omejen spomin za vsako aplikacijo in ostale funkcije, ki lahko šifrirajo, dešifrirajo in podpisujejo paketni prenos podatkov.

Varnostni element se lahko implementira ali v ločen varnostni čip pametne kartice (nanaša se na vgrajen varnostni element), v SIM/UICC (uporabljajo ga GSM mobilni operaterji za avtentikacijo uporabnikov, vzdrževanje njihovih osebnih podatkov ter aplikacij na svojih omrežjih) ali pa v SD karticah, ki se jih lahko vstavlja v mobilne telefone. Pristop implementacije varnostnega elementa je izbran s strani mobilnega operaterja in/ali ponudnika storitev (slednje za implementacijo SD kartic) [16].

3. Regulacija kartičnega plačevanja

3.1. Namen

Kakovost implementacije elektronskih plačilnih instrumentov (plačilnih kartic) v trgovsko podjetje je pogojena z dobrim poznavanjem samih instrumentov ter standardov, ki predpisujejo smernice za poslovanje z njimi. Zato bodo v tem poglavju podrobneje opisane zahteve standarda za kartično plačevanje. Trgovska podjetja morajo zadostiti zahtevam standarda. V primeru neupoštevanja jim lahko grozi odpoved poslovanja z elektronskimi plačilnimi instrumenti. Namen poglavja je, podati odgovornim v organizaciji, ki ima namen vključiti elektronske plačilne instrumente v svoje poslovanje, širšo sliko regulacije elektronskih plačilnih poti. To poglavje daje uvod v bolj eksaktne napotke za trgovska podjetja, ki sledijo v naslednjem poglavju.

3.2. Uvod

Pri navedbi globalnih ponudnikov shem plačilnih kartic (2.2.3.1. Globalni ponudniki shem plačilnih kartic) je bil omenjen standard, ki so ga ustanovile članice Svéta PCI, ki so hkrati tudi glavni akterji v panogi plačilnih kartic.
Svét PCI opredeljuje zahteve oziroma smernice za vse akterje v panogi plačilnih kartic v obliki Standarda varnosti podatkov kartičnega poslovanja (v nadaljevanju in angleška kratica PCI DSS). Skladnost s standardom je obvezna za vsa prodajna mesta (ne glede na velikost in ne glede na način sprejemanja plačilnih kartic), finančne inštitucije ter procesne centre. Osnovno poslanstvo zagotovitve standarda je varnost podatkov imetnikov kartic in njihovih plačil. To z vidika trgovcev pomeni varnost podatkov njihovih strank in s tem zmanjšanje zlorab ter posledično izogib slabi podobi prodajnega mesta.

S strani finančnih inštitucij so interesi po zadostitvi standardu so prav tako veliki. Njihov glavni interes je zmanjšanje možnosti za zlorabe, ki bi sprožile odškodninske zahteve in s tem ogrozile dobro ime.

Ko govorimo o regulaciji kartične industrije, ne moremo mimo ugotovitve, da so zlorabe na bankomatih zelo pogost primer, vendar se lastniki bankomatov (v Sloveniji so to poslovne banke) konkretno ne odzovejo na ta pereč primer, razen s tem, da imajo bankomati nameščene kamere. Ko že pride do suma tovrstnih zlorab (skimming, cash trapping, ...), procesni centri preko svojih aplikacij ugotavljajo morebitne zlorabe, prekličejo kartice, ki so v tem obdobju na tem bankomatu izvajale dvigovanje gotovine. Odprto vprašanje pa ostaja ali bi bilo mogoče bankomate nadgraditi še z varovali, ki bi zaznali namestitev dodatne opreme na zunanjem delu bankomata. Reagiranje na nenavadne transakcije, ki se morebiti zaznajo po zlorabi z branjem podatkov s kartice (skimming) je »gašenje požara«, ko se je kraja podatkov enkrat že zgodila. Kamere, ki so nameščene na bankomatih tudi ne preprečujejo kraje podatkov. Zato, da bi se banke izognile morebitnim tožbam in/ali izgubi ugleda se raje odločajo za preklic kartic.

3.3. Standard PCI DSS

Del kartične industrije, ki je dobro reguliran je tisti z varnostnim standardom PCI DSS in zajema skupek orodij in ukrepov za varno ravnanje z občutljivimi podatki pri kartičnem poslovanju in procesiranju. Temelji standarda so povzeti po zahtevah glavnih ponudnikov kartičnih shem, kot sta MasterCard in Visa.

Trenutno standard predstavlja enoten mednarodni pristop k varovanju občutljivih podatkov in preprečevanju zlorab. Uvedba standarda zagotavlja višji nivo varnosti, ohranjanje zaupanja, zaščito pred škodnimi dogodki in posledično zaščito pred finančnimi izgubami in izgubo ugleda.
Zadostitev standardom se nalaga vsem entitetam, ki kakorkoli prihajajo v stik s plačilnimi karticami (hranjenje, obdelovanje ali prenašanje podatkov o imetnikih kartic ter njihovih transakcijah). To so trgovci, procesni centri, lastniki prodajnih mest in banke. Prvi v verigi plačevanja s karticami so trgovci oz. prodajna mesta, za njimi zaupne podatke dobijo oz. procesirajo procesni centri, ki so vmesni člen med trgovci in bankami.

PCI DSS standard spada v družino PCI standardov.

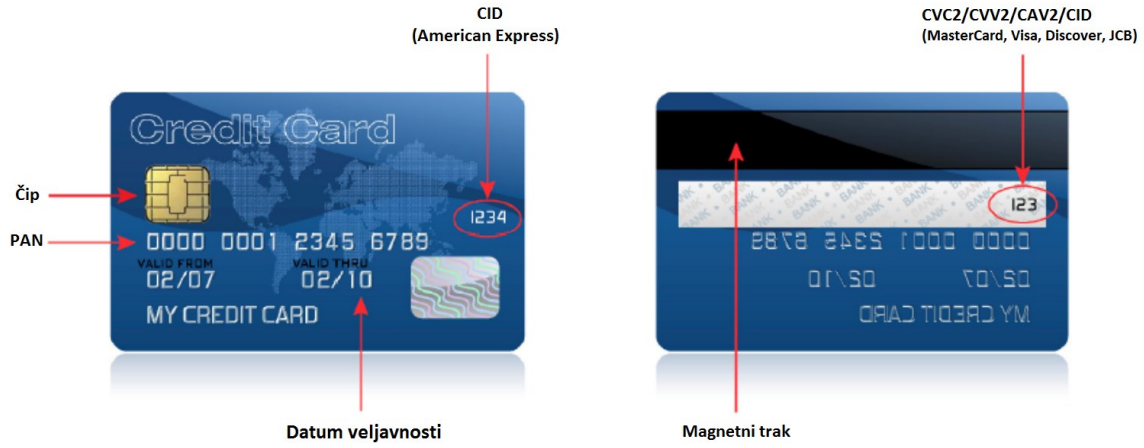
3.3.1. Pojem podatka o imetniku kartice

Pojem o imetniku kartice (ang. Cardholder Data ali CHD) predstavlja skupek varnostno občutljivih podatkov. Najbolj varnostno kritičen podatek je celotna PAN številka (ang. Primary Account Number), ki skupaj z imenom in priimkom imetnika kartice, datumom veljavnosti in servisno številko, predstavljajo CHD podatke [12].
Tako je PAN številka primarni element zaščite in ključni kriterij za uvedbo PCI DSS standarda. V kolikor ga podjetje ali organizacija v svojih sistemih ali omrežjih hrani, prenaša ali procesira se od njega zahteva skladnost s PCI DSS standardom.
Občutljive podatke za overjanje se po izvedbi avtorizacij ne sme shranjevati, tudi v šifrirani obliki ne. Izjema so procesni centri ali druge organizacije, ki zaradi svojega poslovanja oz. dela poslovanja nastopajo v vlogi izdajatelja kartic. Skladno temu su podane dodatne zahteve pri upravljanju teh podatkov. Varovanje PAN številke je lahko izvedeno s »tokenizacijo«, kjer je PAN številka prevedena v neke vrste žeton (ang. token), ki se v taki obliki vodi skozi celoten sistem ali množico sistemov (v podatkovnih bazah) v podjetju do končne točke izhoda iz podjetja. Med občutljive podatke za overjanje uvrščamo podatke z magnetnega traku ali čipa, PIN številko, varnostno koda na kartici ($CAV_2/CVC_2/CVV_2$/CID).

		Podatek	Dovoljeno hranjenje	Zahteva po šifriranju
Podatki o računu	Podatki o imetniku kartice	Številka kartice (PAN)	DA	DA
		Ime	DA	NE
		Servisna koda	DA	NE
		Datum veljavnosti	DA	NE
	Občutljivi podatki za avtentikacijo	Celoten magnetni zapis	NE	Ne, ne sme biti shranjen
		$CAV_2/CVC_2/CVV_2$/CID	NE	Ne, ne sme biti shranjen
		PIN koda	NE	Ne, ne sme biti shranjen

Tabela xx: Varnostno občutljivi podatki in njihovo hranjenje ter obveza po šifriranju skladno s PCI DSS standardom

Podatek naveden v tabeli, se ob izvedbi transakcije prenaša med prodajnim mestom, procesnim centrom, bankami. Navedeno je opisano v poglavju 2.2.1.6 (Procesiranje transakcije na POS terminalu v Sloveniji).



Slika 11. Ključni podatki na plačilni kartici
Vir: **Stran Združenja bank Slovenije:** Smernice za prodajna mesta – trgovce [9]

3.3.2. Zahteve in smernice standarda

Zadnja objavljena verzija je *V3.2 – APR 2016*.

Zahteve standarda so opredeljene v šestih področjih. Standard je opredeljen z dvanajstimi zahtevami. [11]:

Vzpostavitev in vzdrževanje varnega omrežja

1. **Zahteva: Namestite in vzdržujte protipožarne pregrade z namenom varovanja imetniških podatkov**

Obstoječo konfiguracijo moramo dokumentirati in opremiti s shemo omrežja, ki jasno prikazuje vse povezave do podatkov o plačilnih karticah. Dokumentacija mora vsebovati obrazložitev uporabe vsake storitve v omrežju (FTP, SNMP, Telnet, ipd.). Vsaka naprava, priklopljena v notranje omrežje z dostopom do interneta, mora imeti nameščeno lastno protipožarno pregrado[12].

Polletni pregled pravil protipožarnih pregrad. Upravičena mora biti uporaba vsakega protokola razen (http, TLS, SSH in VPN), še posebej manj varnih (FTP), za katere morajo biti opisane tudi ustrezne varnostne zahteve.

2. **Zahteva: Ne uporabljajte začetnih gesel in varnostnih postavk proizvajalca programski opreme**

   Pred priklopom sistema v omrežje moramo odstrani vsa privzeta gesla in skrbno pregledati vse privzete nastavitve. [12].

   Vse začetne vrednosti programskih paketov so dobro znane računalniškim skupnostim in zaradi tega pomenijo veliko tveganje. Vzpostavljeni morajo biti lastni konfiguracijski standardi, ki morajo upoštevati odpravo znanih varnostnih pomanjkljivosti v operacijskih sistemih, podatkovnih bazah in aplikacijah.

Varovanje podatkov imetnikov kartic

3. **Zahteva: Zaščitite shranjene podatke o plačilnih karticah**

   Kodiranje varnostno ključnih podatkov o imetniku kartice je pomembna komponenta zaščite, ki preprečuje razkritje tudi v primeru vdora ali kraje podatkov. Poleg kodiranja obstajajo še drugi načini varovanja podatkov – tokenizacija, maskiranje in drugi načini. Doba hranjenja podatkov o plačilnih karticah naj bo minimalna, njihovo uničenje pa naj bo podprto s preverjenimi in zanesljivimi postopki. Avtentikacijski podatki naj ne bodo po opravljeni uspešni avtentikaciji shranjeni nikjer. Nekateri podatki, kot so številke PIN (Personal Identification Number) in CVV (Card Verification Code) naj ne bodo nikoli shranjeni[12].

4. **Zahteva: Šifrirajte podatke imetnikov kartic pri prenosu v odprtih, javnih omrežjih**

Zahtevana je uporaba močnega šifriranja in varnih protokolov IP-SEC, SSL/TLS, SSH pri prenosu podatkov skozi odprta, nezaščitena omrežja [12].

Pri ugotavljanju skladnosti z zahtevo preverimo, če se šifriranje uporablja pri prenosu, če se imetnikovi podatki zahtevajo šele po vzpostavitvi povezave in tudi preverimo sprejem samo zaupanja vredne TLS certifikate. Transakcije preverimo tako, da spremljamo njihov potek in kodiranje podatkov pri prenosu.

Vzdrževanje programa upravljanja ranljivosti

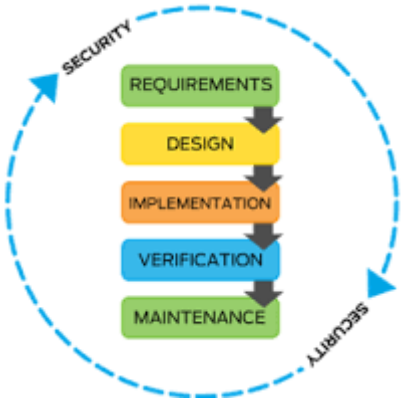
5. Zahteva: Uporabljajte in redno posodabljajte protivirusne zaščite in protipožarno programsko opremo

Vsi sistemi, ki so podvrženi grožnjam s spleta morajo imeti nameščeno protivirusno in protipožarno programsko opremo [12] in mora biti nameščena na vse komponente sistema, ki so izpostavljene možnim okužbam. Zaščita se priporoča, poleg preprečevanja, odkrivanja in odstranjevanja virusov, tudi proti zlonamernemu programju.

Protivirusna zaščita se mora redno posodabljati, mora biti ves čas aktivna in mora beležiti dnevnike aktivnosti.

6. Zahteva: Razvijajte in vzdržujte varne sisteme in aplikacije

Zagotovite, da imajo vsi sistemi nameščene zadnje varnostne popravke, identificirajte grožnje, razvijajte »varno« programsko opremo v skladu s SDLC (ang. Software Development Life Cycle), bolj natančno s S-SDLC (ang. Secure - SDLC). Lastna programska oprema mora biti revidirana s strani kvalificiranega osebja, ki samo ne sme biti avtor opreme, lahko pa je to zaposleni v podjetju [12].



Slika 12: Grafični prikaz življenjskega cikla razvoja programske opreme

Kritični varnostni popravki se morajo na izpostavljene sisteme namestiti v roku enega meseca od uradne objavljene izdaje. Pregledajo in preverijo se roki za namestitev popravkov, odvisni od kritičnosti in izpostavljenosti komponente. Skrbniki sistemov so zavezani k rednemu spremljanju pojava novih varnostnih groženj in njihovi obravnavi skladno s politiko družbe.

- Spremembe konfiguracij in varnostne popravke testiramo pred namestitvijo v produkcijo
- Produkcijska okolja so ločena od ostalih (razvojnih, testnih, simulacijskih)
- Nujna je delitev dela zaposlenih po okoljih in omejitve dostopov
- Produkcijski podatki ne smejo, razen v maskirani obliki, prehajati iz produkcije na ostala okolja
- Testne podatke in uporabnike je potrebno odstraniti pred prehodom v produkcijo
- Pred aktivacijo programske opreme v produkciji je potrebno odstraniti vse lastne račune
- Pred aktivacijo programske opreme v produkciji izvedemo pregled kode

Dobra praksa: Pri razvoju programske kode se poslužujemo uporabe parametrov, ki vrednosti pridobivajo iz okolijskih datotek (konfiguracij), ki so različne po okoljih. Sama programska koda se med prepisi iz razvojnega, testnega, simulacijskega in produkcijskega okolja ne spreminja.

Vzpostavitev ustreznih pristopnih kontrol

7. Zahteva: Omejite dostop do podatkov imetnikov kartic

Zaposleni naj imajo dostop le do podatkov, ki jih potrebujejo za nemoten delovni proces (ang. need-to-know). Vpeljava sistema za nadzor nad dostopi in dosledno dodeljevanje pravic uporabnikom mora biti zagotovljena [12]. Politiko dostopa se gradi po principu »prepovedano, če ni eksplicitno dovoljeno«.

8. Zahteva: Določite enolične identifikacije osebam z dovoljenim dostopom do podatkov imetnikov kartic

Omogočena mora biti sledljivost vsem uporabnikom sistema v vsakem trenutku. Za dostop do notranjega omrežja od zunaj naj se uporabi dvofaktorska avtentikacija in dobra politika upravljanja z gesli uporabnikov. Gesla morajo biti vseskozi hranjena v šifrirani obliki (uporaba zgoščevalnih funkcij, ang. Hash Algorithm) [12]. Posredovanje gesel je omogočeno le na zaščiten način. Uporabniška imena in gesla naj ne bodo prednastavljena, skupinska ali znana širšemu krogu zaposlenih. Gesla se morajo menjati najmanj vsakih 90 dni, dolžin gesla naj ne bo krajša od 7 znakov (predpisana je prisotnost črk in številk). Geslo se ne sme ponoviti iz zgodovine vsaj štirih gesel. Uporabnik ima največ 6 možnih neuspešnih poskusov za prijavo.

Redni nadzor je potreben nad vnosom, spremembami in brisanji uporabnikov, ki jih lahko izvaja le avtorizirana oseba.

9. Zahteva: Omejite fizične dostope do sistemov s podatki imetnikov kartic

Vse vstopne točke do sistemov in aplikacij naj bodo nadzorovane, vključno z omrežnimi vtičnicami. Obiskovalci in zunanji pogodbeni izvajalci morajo biti v prostorih podjetja ustrezno vizualno označeni (značke, priponke, idr.) in s tem prepoznavni med zaposlenimi, ki morajo prav tako imeti priponke.

Zagotovljeno mora biti fizično varovanje vseh medijev (dokumentov, prenosnih medijev, idr.), njihova ustrezna klasifikacija in uničenje [12]. Opredeljena mora biti klasifikacija zaupnosti medijev glede na občutljivost podatkov. Mediji, ki vsebujejo podatke o imetnikih kartic morajo biti zaščiteni in varno shranjeni. Prenos iz varnega območja mora biti ustrezno nadzorovan, izvede se lahko le na avtoriziran in varovan način. Uničenje medijev mora biti na način, da ni mogoča kasnejša rekonstrukcija podatkov.

Redni nadzor in preizkušanje omrežja

10. Zahteva: Spremljajte vse dostope do omrežnih virov in podatkov o plačilnih karticah

Rekonstrukcija dogodkov na podlagi zapisov v sistemskih dnevnikih, sinhroniziran čas po vseh strežnikih, preverjanje integritete datotek na sistemu, dnevno spremljanje dnevniških zapisov [12]. Skratka, zagotovljena mora biti revizijska sled za primer rekonstrukcije dogodka. Sled mora biti berljiva in zato mora vsebovati uporabniško ime, tip aktivnosti, status uspešnosti, izvor dogodka in podatek ali komponento, ki ga dogodek zahteva. Revizijske sledi je potrebno tudi ustrezno zaščititi pred morebitnimi spremembami ali brisanji ter hraniti za obdobje najmanj enega leta.

Dobra praksa: Zaradi performančnih in kapacitetnih obremenitev podatkovnih baz po vključitvi funkcionalnosti sledenja vseh dostopov do podatkov, omejimo beleženje le na dostope osebnih uporabnikov.

11. Zahteva: Redno izvajajte varnostne preglede sistemov, preverjajte varnostne programov in procesov

Vsaj vsako četrtletje naj se izvede notranji in zunanji varnostni pregled, vsaj enkrat letno in po vsaki bistveni spremembi IKS pa naj se izvede tudi temeljito penetracijsko testiranje, vključno s pregledom brezžičnih točk [12].

Najmanj vsake tri mesece - Potrebno je opraviti preglede ranljivosti iz zunanjega sveta (internet) ter notranje (lokalno omrežje) z varnostnim pregledom po vsaki večji spremembi (dodajanje ali spreminjanje komponent sistema, ob spremembah sheme omrežja ali ob spremembah pravil protipožarne pregrade). Potrebno je izvesti pregled brezžičnih omrežij.

Najmanj enkrat letno ali ob večji spremembi sistema - Izvedba penteracijskega testa, ki zajema poskuse vdora v sistem iz notranje in zunanje strani.

Dobra praksa: Testiranje vdora naj izvajajo različna kvalificirana podjetja.

Vzdrževanje varnostne politike

12. Zahteva: Vzpostavitev varnostne politike za zaposlene in pogodbene izvajalce

Verjetno najpomembnejša zahteva govori o vzpostavitvi varnostne politike, ki zajema vse zahteve PCI DSS. Vzpostaviti je potrebno dnevne postopke osnovnih pregledov informacijskih sistemov. Ne smemo pozabiti na zasebne naprave zaposlenih (npr. telefone, ki jih ti prinašajo v podjetje in vklapljajo v notranje omrežje). Izobraževanja zaposlenih o varnostni politiki, preverjanje znanja in seznanjanje z grožnjami [12]. Ob varnostnih incidentih morajo biti vzpostavljeni postopki, ki jasno opredeljujejo vloge in odgovornosti. Postopki morajo zajemati vsaj enkrat letno preizkušanje.

Dobra praksa: Simulacija incidenta in izvedba prehoda na rezervno lokacijo, razpoložljivost ljudi, usposabljanje odgovornih, reagiranje na alarme, idr.

3.3.3. Preverjanje skladnosti s standardom

Skladnost s standardom se zahteva na vseh področjih, ugotavlja se z lastnim ocenjevanjem (ang. Self-Assesment Questionaire ali SAQ) ali s pregledi kvalificiranega varnostnega presojevalca iz področja kartične industrije (ang. Oualified Security Assessor ali QSA). Certifikat z uradnim nazivom *Certificate of PCI DSS Compliance* podjetje pridobi enkrat, potem pa ga mora letno obnavljati in zadostiti novim zahtevam v samem standardu ali pa ob morebitnih spremembah v operativnem okolju podjetja. Kvalificirani presojevalec varnosti je oseba, ki je verificirana s strani Svéta PCI SSC. Skladnost s standardom za finančne institucije je pogoj za poslovanje.

4. Smernice za uvedbo standarda PCI DSS za prodajna mesta

4.1. Namen

V prejšnjem poglavju smo opisali zahteve standarda, ki veljajo splošno, za vse deležnike v verigi kartičnega poslovanja. Trgovska podjetja z enim ali množico prodajnih mest so poleg potrošnika ključne entitete za izvedbo plačilne transakcije. Ko se prodajno podjetje sooči z zahtevami po posodobitvi svojih prodajnih poti (npr. uvedba spletne prodaje), mora v svoje plačilne instrumente (če jih še nima) vključiti tudi elektronske načine plačevanja (plačilne kartice). Omenjeno je bilo že, da mora za tovrstna plačila slediti zahtevam standarda PCI DSS. Cilj tega poglavja je predstaviti odgovornim v takih organizacijah prednosti upoštevanja smernic, korake za zagotovitev skladnosti ter napotke za izvedbo samoocenitve.

4.2. Prodajna mesta

Trgovska podjetja - trgovci so pod velikim pritiskom iskanja konkurenčnih prednosti ali vsaj sledenju trendom, ki jih narekuje neusmiljen trg. To velja za vsa trgovska podjetja ne glede na tržišče ali prodajne produkte. Potrošniki (v kontekstu tega poglavja - imetniki plačilnih kartic) postajajo zahtevnejši. Trgovska podjetja se morajo odzvati na zahteve potrošnikov po sodobnejših načinih nakupov in sodobnejših oblikah plačevanja na prodajnih mestih. Prodajna mesta v trgovskem podjetju ali pri trgovcu niso omejena le na fizične lokacije. Ravno nasprotno, pojem »sodobnost« zajema hitre, enostavne, varne ter časovno in lokacijsko neomejene nakupne in plačilne transakcije.

Za trgovce oz. prodajna mesta veljajo enake zahteve PCI DSS standard s tem, da je poudarek v nekaterih točkah večji oz. v drugih manjši. Tudi preverjanje skladnosti se izvaja drugače. Vsekakor pa je skladnost s standardom bistvenega pomena za vsa prodajna mesta. Velja za vse trgovce in prodajna mesta, ki sprejemajo plačilne kartice, pa naj si gre za velike svetovne korporacije, manjše trgovce ali pa za majhne spletne trgovine ter tudi neodvisno od tega, ali je

njihovo poslovanje v online ali offline načinu. Razlikujejo se zahteve za skladnost s PCI DSS standarda odvisno tudi od obsega poslov, ki jih določajo posamezne kartične sheme (MasterCard, Visa, American Expres, …) in ne Svét PCI.

Standard PCI DSS zagotavlja informacije, izobraževanje in usposabljanje tako za prodajna mesta kot tudi za presojevalce skladnosti. PCI DSS je nastal z uskladitvijo varnostnih programov kartičnih shem Visa in MasterCard.

4.3. Prednosti uvedbe standarda za prodajna mesta - trgovce

Uvedba standarda ima za prodajna mesta veliko prednosti, po drugi strani neupoštevanje smernic lahko privede do negativnih posledic. Trgovci in prodajna mesta so velikokrat tarča napadov in zlorab podatkov o kartici. Naloga prodajnih mest je, da zaščitijo te podatke. V primeru morebitne kraje podatkov na kartici lahko trgovca doleti kazen ali mu je odvzeta pravica do poslovanja oz. sprejemanja plačilnih kartic. Skladnost s standardom spodbuja vse trgovce s prodajnimi mesti, na katerih hranijo, posredujejo ali obdelujejo občutljive podatke kartičnega poslovanja. Skladnost s PCI DSS zmanjšuje finančna tveganja. Skladnost s standardom ne preverja Svét PCI, kakor tudi ne predvideva ukrepov neupoštevanja zahtev. Za to so zadolžene kartične sheme. Ob neupoštevanju so predvideni finančni ukrepi, oziroma v skrajnih primerih prepoved poslovanja oz. sprejemanja plačilnih kartic. Posamezne kartične sheme sàme določajo zahteve za skladnost. To, katere zahteve je potrebno zagotavljati, mora trgovec sam preverjati pri banki pridobiteljici prodajnih mest (banka trgovca) [10].

4.4. Kako zagotoviti skladnost?

PCI DSS je skupek tehničnih in operativnih zahtev za zaščito podatkov imetnika kartice, ki jih je predpisal Svét PCI.

KORAKI:

1. Opredelitev ocene, kjer trgovci definirajo, kje se občutljivi podatki kartičnega poslovanja hranijo, obdelujejo ali prenašajo. Sledi popis infrastrukture in poslovnih procesov, ki se jih kartično poslovanje dotika. Pripravi se ocena tveganja in pregled ranljivih točk za varnost občutljivih podatkov pri kartičnem poslovanju.
2. Odprava pomenljivosti, ter ukrepanje za umik oz. ne shranjevanje občutljivih podatkov kartičnega poslovanja.

3. Izpolnitev poročila o skladnosti prodajnega mesta. S poročilom o skladnosti s PCI DSS mora trgovec seznaniti banko lastnico POS terminala, s katero trgovec posluje.

Odvisno od obsega letnega poslovanja trgovca, posamezne kartične sheme opredeljujejo obseg ukrepov za doseganje skladnosti s PCI DSS. Kot primer, se pri trgovcu, čigar letni obseg poslovanja presega 6 milijonov transakcij, zahteva skladnost s standardom, ki je opredeljena v kategorijo Raven 1 in zahteva:

- Letno presojo skladnosti trgovca na njegovi lokaciji, opravi jo verificiran presojevalec QSA
- Četrtletno preverjanje varnostnih ranljivosti informacijske podpore, ki ga opravi ASV(podjetje pooblaščeno za izvajanje zunanjih varnostnih ranljivosti)

Za trgovce z manjšim obsegom letnih transakcij velja upoštevanje predpisanih zahtev na Raven 2, Raven 3 ,… Tako pri manjših trgovcih poteka preverjanje z letno samooceno s pomočjo samoocenitvenega vprašalnika PCI DSS (SAQ), četrtletno preverjanje varnostnih pomanjkljivosti in posredovanje potrdila o skladnosti.

Vse kartične sheme imajo podobno klasifikacijo in podobne zahteve, odvisno od obsega letnih transakcij.

4.5. Samoocenitveni vprašalnik PCI DSS

Samoocenitveni vprašalnik PCI DSS – SAQ je vprašalnik, namenjen za trgovce, ki niso zavezani k pregledovanju skladnosti s strani pooblaščenih presojevalcev. Namen vprašalnika je pomoč pri pridobitvi samoocene skladnosti s PCI DSS. Pri tem je trgovec zavezan, da z oceno seznani banko lastnico POS terminala. Obstaja več tipov samoocenitvenih vprašalnikov. Izbira, na katerega bo trgovec odgovarjal, je odvisna od tega, na kakšen način trgovec izvaja transakcije s plačilnim karticami, ter katere tehnološke rešitve uporablja. Trgovec mora na vprašanja odgovoriti z DA ali NE [10].

Tip SAQ	**Na kateri način trgovec izvaja transakcije s plačilnimi karticami?**
A	Vse procese, povezane s podatki imetnikov plačilnih kartic, opravljajo zunanji izvajalci. Ne izvaja se elektronsko shranjevanje, obdelava ali prenos podatkov o imetnikih plačilnih kartic.

B	Imprinterji ali samostojni klicni terminali. Podatki o imetnikih plačilnih kartic se ne shranjujejo elektronsko.
C-VT	Spletni virtualni terminali. Podatki o imetnikih plačilnih kartic se ne shranjujejo elektronsko.
C	Plačilna aplikacija je povezana v internet. Podatki o imetnikih plačilnih kartic se ne shranjujejo elektronsko.
D	Vsa preostala prodajna mesta, ki niso opredeljena v zgoraj navedenih tipih in drugi ponudniki plačilnih storitev.

5. Metodologija uvedbe spletne prodaje v trgovsko podjetje

5.1. Namen

V začetnem poglavju smo skozi opise prisotnih plačilnih instrumentov in ozadje finančnih transakcij podali vpogled v širok nabor plačilnih možnosti. V osrednjem delu je bila opisana regulativa najbolj zastopanega in obetajočega plačilnega instrumenta. V sklopu tega je bil podan kratek povzetek prilagojene regulative za trgovska podjetja. Na osnovi teh poglavij se lahko trgovska podjetja odločajo za posodabljanje svojega poslovanja skozi korake, ki so opisani v tem poglavju.

5.2. Uvod

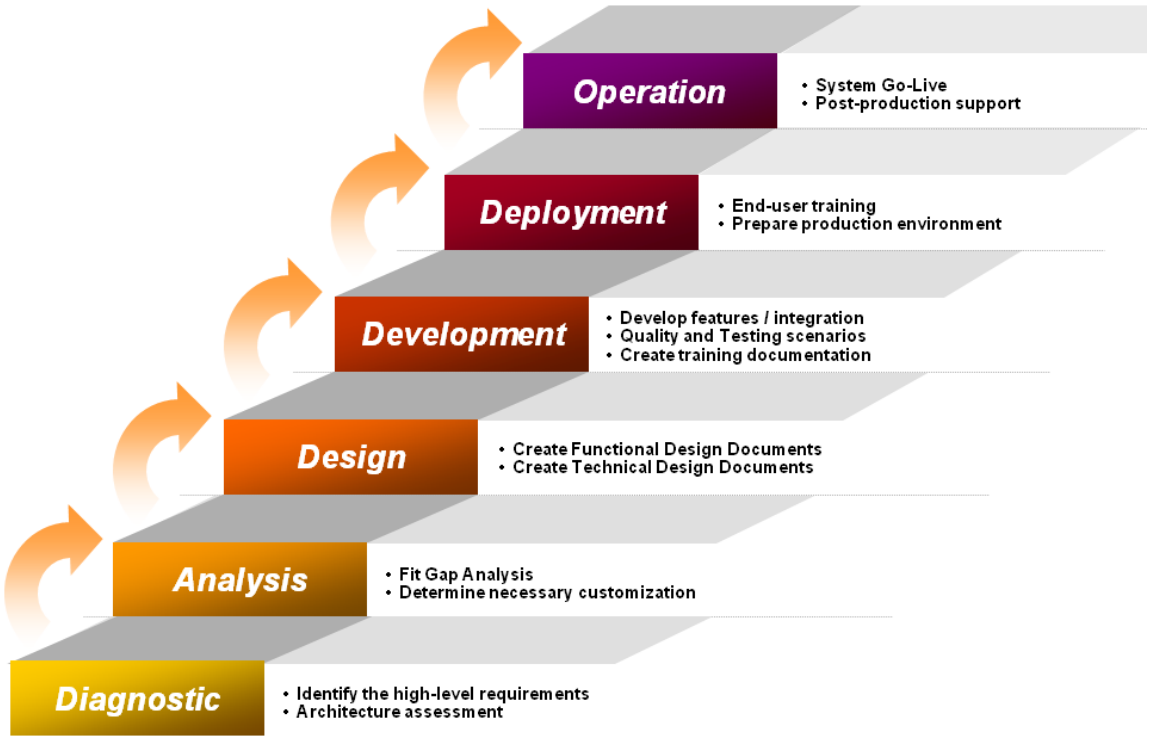
Vsa trgovska podjetja množično uvajajo spletno prodajo kot alternativo fizični prodaji v trgovinah, ter kot odziv na spremenjene navade in zahteve potrošnikov. Poleg dokaj velikih investicijskih stroškov pri vpeljavi, se na daljše obdobje pokaže velika množica prednosti z integracijo spletne prodaje v trgovskem podjetju (delovni čas ni omejen, zmanjšanje stroškov povezanih z prodajalci, izložbami, tudi za velike korporacije en informacijsko komunikacijski sistem, centralizacija skladišča in še množica drugih).

Preden se trgovec odloči za vpeljavo spletne prodaje, si mora odgovoriti na nekaj ključnih vprašanj s katerimi opredeli predpogoje in smeri za realizacijo [13]:

1. Ali ima družba registrirano dejavnost trgovine za prodajo prek spleta?
2. Kako bodo izdelki dostavljeni kupcem?
3. Na kakšen način bo katalog izdelkov predstavljen v spletni trgovini?
4. Kako naj bo predstavljena spletna trgovina?
5. Katere možnosti plačevanja bodo na razpolago kupcem?
6. Ali ima družba urejene vse pravne zahteve za spletno prodajo?
7. Kako in s katerimi orodji naj se izvajajo statistike spletne prodaje?

8. Ali je zaključen postopek registracije domene?

Metodologija uvedbe opredeljuje običajen pristop izvedbe korakov za implementacijo [14] spletne prodaje v trgovsko podjetje.



Slika 13: Grafični prikaz Microsoft Sure Step metodologije [17]
Vir: BSE Consulting

5.3. Postopki uvedbe spletne prodaje

Proces uvedbe spletne prodaje v trgovsko podjetje opredelimo v obvladljive faze ali korake. Vsaka faza za svoje delovanje in potek potrebuje deležnike, ki aktivno sodelujejo v realizaciji in uresničevanju ciljev in za to deležniki potrebujejo vhodne izdelke (dokumenti ali informacije) in orodja (aplikacije, oprema, sredstva). Koraki ali faze so opredeljeni v točke:

1. **Pregled in analiza obstoječih prodajnih poti [P1] – (ang. DIAGNOSTIC)**
   V prvem koraku diagnosticiranja trenutnih prodajnih poti želimo opredeliti ekonomsko upravičenost vpeljave novih prodajnih poti. Za ta rezultat je potrebna vključenost vodstvenih kadrov, plansko-investicijskih služb ter kadrov, ki so neposredno vključeni v vzdrževanje in delovanje ključnih prodajnih procesov (aplikativni skrbniki, tehnologi, analitiki, varnostni inženirji).

2. **Opredelitev obstoječe poslovno-informacijske arhitekture [P2] – (ang. ANALYSIS)**
   Iz obstoječe dokumentacije, vprašalnikov ali celo iz nadzornih sistemov poskušamo ustvariti sliko poslovno-informacijske arhitekture. V tem koraku je nujna prisotnost organizacijske sheme ter sheme omrežij, popis obstoja strojne opreme in njihova povezljivost, prisotnost programske opreme, idr. Rezultat tega koraka je popis »as-is« ter zaključena analiza obstoječe poslovne-informacijske arhitekture.

3. **Opredelitev zahtev za realizacijo uvedbe spletne prodaje [P3] – (ang. DESIGN)**
   V tretjem koraku opredelimo oz. oblikujemo zahteve, ki bodo privedle do vpeljave spremembe v obstoječe poslovanje in njene ekonomske upravičenosti. Konkretne rešitve morajo biti sodobne (potrošnikom zanimive) ter hkrati uveljavljene z vidika varnosti, stabilnosti ter odzivnosti. V pomoč pri tem koraku nam pridejo odgovori na vprašanja ki smo jih navedli v začetku poglavja.

4. **Izbira obstoječih rešitev ali razvoj novih [P4] – (ang. DEVELOPMENT)**
   Potem, ko imamo opredeljene zahteve in smernice, pričnemo z izbiro najprimernejše rešitve. Lahko se odločimo za notranji razvoj, nakup standardizirane rešitve ali podajanje zahteve za razvoj zunanjim izvajalcem. Odločitev, za katero pot se bomo odločili, je odvisna od vrste dejavnikov – razpoložljivi resursi, časovne zahteve končanja projekta, stroškovni vidik investicije, idr.

5. **Integracija novih rešitev v poslovno-informacijsko arhitekturo [P5] - (ang. DEPLOYMENT)**
   V koraku integracije morajo biti odgovori na vprašanja iz začetka poglavja jasno opredeljena in zahteve realizirane. V tem koraku so vidne spremembe na poslovno-informacijski arhitekturi. Spremembe so vidne v procesni shemi, ki mora biti dograjena z novimi procesi. Prav tako morajo biti realizirane predvidene organizacijske spremembe. Z namenom realizacije zadnje faze je potrebno ustrezno dokumentirati celotno poslovno-informacijsko arhitekturo. Nikakor se ne sme pozabiti na izobraževanje in osveščanje zaposlenih o novih zahtevah, smernicah, ter novih rešitvah, ki smo jih vpeljali.

6. **Priprava načrta vzdrževanja novo vpeljanih rešitev [P6] - (ang. OPERATION)** Zadnja faza v postopku je lahko zelo enostavna in trivialna, če smo v zaporednih korakih ustrezno dokumentirali posnetke stanj ter vpeljane spremembe. V tej fazi je potrebno sestaviti postopke in navodila za reagiranje ob izjemnih postopkih kot so izpadi ter prekinitve v delovanju sistema. Nikakor se ne sme pozabiti na izobraževanje in osveščanje zaposlenih o novih zahtevah, smernicah, ter novih rešitvah, ki smo jih vpeljali.

5.4. Ključne vloge pri fazah vpeljave spletne prodaje

Osebe, ki so vključene v aktivnosti oz. deležniki na projektu vpeljave spletne prodaje opredelimo v vloge:

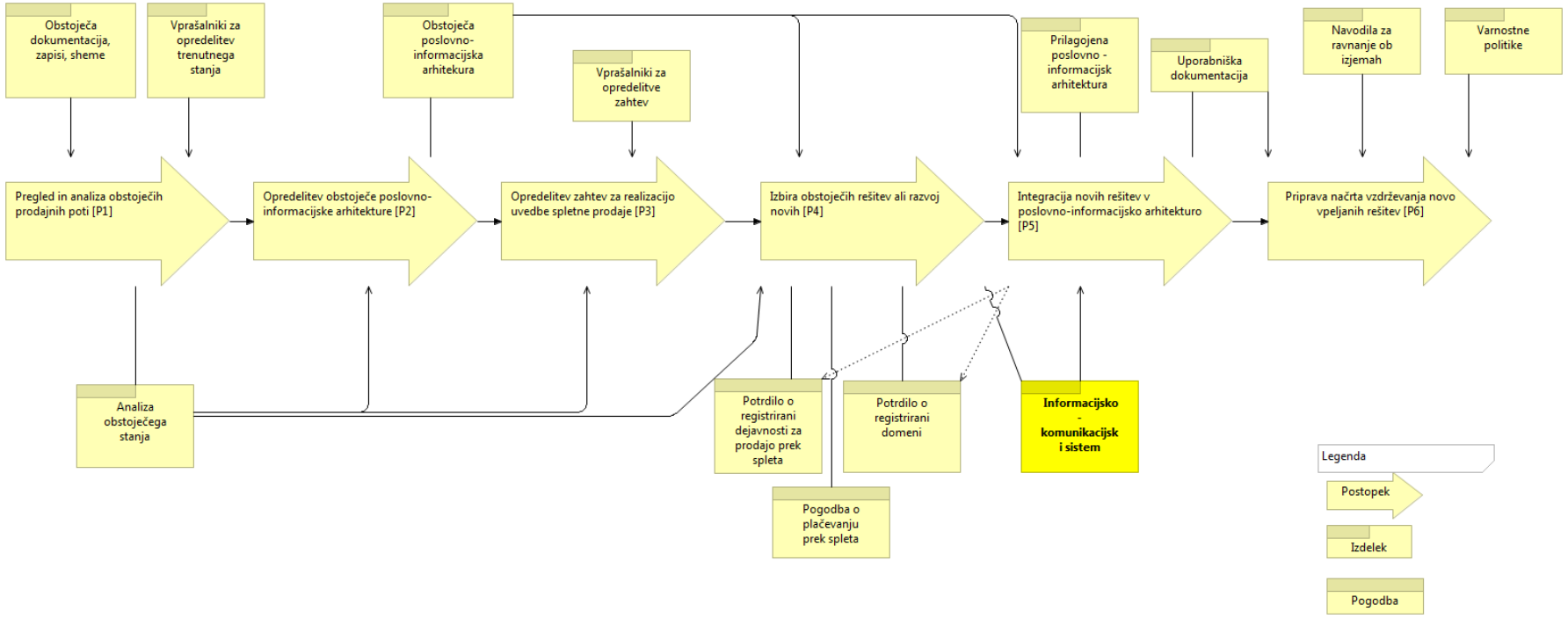
Skrbnik informacijskega sistema	Člani te vloge pripravijo ustrezna strojna in programska orodja, zagotavljajo delovanje strojne in programske informacijske opreme, svetujejo pri uporabi in nadgradnji informacijskih sistemov, vodijo predpisano dokumentacijo, pripravljajo manj zahtevne ponudbe za naročnika, zagotavljajo nemoteno delovanje in vzdržujejo informacijsko opremo. [18]
Poslovni analitik	Poslovni analitik je osrednja operativna funkcija na projektu, saj sodeluje v vseh fazah projekta preko izdelave strateškega plana, analize podatkov o poslovno-informacijskem procesu ter arhitekturi. Opredeljuje ga znanje o poslovni strategiji, uporabnikih nove predlagane prodajne rešitve ter obstoječi poslovno-informacijski arhitekturi.
Predstavnik vodstva	Je oseba z visoko stopnjo avtoritete in tisti, ki že v začetni fazi odloča o ekonomski upravičenosti projekta izboljšave nekega poslovnega procesa, saj je taka oseba v podjetju po navadi odgovorna za rezultate poslovanja, na katere je vezan praktično celoten poslovni proces v podjetju. V okviru vloge na projektu, se ta velikokrat prepleta z vlogo sponzorja, ker se od vodstvenih delavcev pričakuje, da z dobrim

	poznavanjem svojega poslovnega področja bistveno prispevajo k kvalitetni izvedbi projekta.
Predstavnik pravne službe	Predstavnik pravne službe mora biti dobro seznanjen s pravnimi zahtevami poslovanja prek spleta. Predpisi s tega področja zajemajo zakone: Obligacijski zakonik (OZ); Zakon o avtorski in sorodnih pravicah (ZASP) Zakon o bančništvu (ZBan-1) Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) Zakon o elektronskem poslovanju na trgu (ZEPT) Zakon o elektronskih komunikacijah (ZEKom) Zakon o gospodarskih družbah (ZGD-1) Zakon o medijih (ZMed) Zakon o trgovini (ZT)
Predstavnik marketinga	V to vlogo spadajo osebe iz oddelka marketinga in so v okviru projekta pomembne z vidika podajanja informacij, zahtev in pričakovanj strank oziroma kupcev podjetja. Navedeno pomembno vpliva na oblikovanje potrošniku prijaznih aplikacij.
Varnostni inženir	Je ključna vloga pri zagotavljanju upoštevanja standardov varnosti s področja IT. Je tisti, ki mora dobro poznati in kritično oceniti vsa varnostna tveganja, ki obstajajo ali bi se lahko pojavila v okviru projekta. Je nepogrešljiv člen pri

	razvoju IT rešitve kot ključni vir pri ocenjevanju procesa z vidika informacijske varnosti, ker zmožnost zagotavljanja ustrezne varnosti procesa lahko bistveno vpliva na izbiro tehnološke rešitve. Izvaja varnostne ukrepe na področju informacijskih sistemov ter izvaja politiko gesel.
Tehnološki analitik	V to vlogo spada oseba, ki dobro pozna obstoječe IT rešitve, trende in novosti na IT področju in je ključna vloga pri izbiri ustrezne IT rešitve za projekt (po navadi notranji informatik). Sodeluje že v začetnih fazah projekta, ker je tisti, ki pozna domet obstoječe informacijske tehnologije v podjetju.
Notranji uporabnik aplikacije	To vlogo predstavljajo zaposleni, ki skrbjo za koordinacijo, komunikacijo in pomoč strankam. Po navadi sodeluje pri izdelavi strateškega plana, razvoju in implementaciji aplikativnih sistemov z vidika uporabnika ter z ostalimi vlogami na projektu (poslovni in tehnološki analitik).

5.5. Shema procesa uvedbe spletne prodaje

V spodaj navedeni procesni shemi so skozi faze ali aktivnosti definirani vhodni izdelki, ki so lahko dokumenti, aplikacije ali rešitve. V fazah P4 in P5 (faze realizacije) se sklepajo pogodbe, ki so pogoj za implementacijo rešitve ter pričetek življenjskega cikla aplikacije za spletno prodajo. Po končani implementaciji ne smemo pozabiti, da se morajo informacijske rešitve nenehno spremljati, nadgrajevati in prilagajati zakonskim predpisom (npr., uvedba davčnih blagajn) ter varnostnim smernicam. S pričetkom uporabe spletne prodaje in uporabe sodobnih plačilnih instrumentov se morajo skrbniki sistema zavedati nenehnih groženj zlorab plačilnih kartic in elektronskih instrumentov, ki so vključeni v spletno prodajo (PayPal, Moneta, plačila s kreditnim karticami).



Slika 14: Shematski prikaz postopka uvedbe spletne prodaje v trgovsko podjetje

Vir: Lasten

6. Sklepne ugotovitve

Sodobni plačilni instrumenti potrošniku omogočajo hitro, enostavno in preprosto porabo (svojih) denarnih sredstev. Uporaba plačilnih kartic je najbolj zastopan plačilni instrument. Vprašanje časa je kdaj se bo medij za plačevanje iz plastičnih kartic prestavil na mobilne naprave. Tehnologija, ki to omogoča je že razvita in prisotna v obliki brezstičnih plačilnih kartic. Finančne institucije bodo morale v kratkem odgovoriti na vse večje povpraševanje po teh spremembah in nadgraditi tudi bančne avtomate. Na strani trgovcev (prodajna mesta) pa se že omogočajo brezstična plačevanja z NFC protokolom.

Osnove smernic za nadzor, varnost in enotnost kritičnih podatkov so predpisane v že sedaj v obvezujočih smernicah za kartično poslovanje – standard PCI DSS.
Skozi nalogo in raziskavo standarda PCI DSS, ki ga informatik oz. tisti, ki ga implementira v neko informacijsko komunikacijsko okolje, mora poznati (naj si bo to finančna institucija ali trgovinsko podjetje), sem prišla do zaključka, da je standard zelo usmerjen v zaščito podatkov o imetniku kartice pred možnimi zlorabami znotraj organizacije. Po drugi strani pa smo priča množičnim zlorabam in krajam denarja na bančnih avtomatih in te so še v porastu. Iz tega je možno sklepati, da objava varnostnih standardov s strani Sveta PCI še ne pomeni, da so naša finančna sredstva varna.

Velika množica plačilnih instrumentov in nenehni razvoj v smeri lažje dosegljivosti, enostavnosti in hitrosti ter relativno množični umik gotovinskih plačil daje sklepati, da je velik interes vseh neposrednih akterjev (globalni ponudniki kartičnih shem, banke, trgovci, procesni centri) in posrednih kot so nacionalna gospodarstva, po takih oblikah denarnih transferjev. Elektronska plačilna sredstva so z vidika teh »interesnih entitet« nadzorovana in upravljana. Zato poenostavljeno povedano, vsakič, ko imetnik finančnih sredstev, pa naj nastopa v vlogi potrošnika, komitenta ali državljana, izvede negotovinsko transakcijo, se delež te zajame v obliki provizij ali davkov.

PCI DSS standard, ki je obvezujoč za vse udeležence, ki poslujejo s plačilnim karticami ali na kakršenkoli način pridejo v stik s podatki o imetniku kartice, z vpeljavo predpisanih zahtev v podjetje (finančna institucija ali trgovinsko - ne glede na velikost), zahtevajo veliko dodatnih resursov. To v času velikih pritiskov s strani lastnikov po zmanjšanju stroškov dela, ni nezanemarljiv dejavnik. Nedvomno vpeljava standardiziranih ter enotnih postopkov v

poslovanje dolgoročno prinaša množico prednosti. Najbolj pa pomanjkanje resursov ob implementaciji sprememb, ki se jih zahteva s standardom, občutijo manjše organizacije (manjši trgovci), ki v svojih organizacijskih strukturah nimajo zadostno usposobljenega kadra, ki bi moral biti vključen ta proces. Če temu dodamo še nujno sledenje trendom po vpeljavi sodobnih prodajnih poti, ki jih prinaša neprizanesljiva konkurenca na vseh tržiščih in v vseh panogah, ugotovimo s kako velikimi preprekami se srečujejo prodajna podjetja. Mogoče je sklepati, da je edina prava pot za napredek takih organizacij vlaganje v ključne resurse, izbira standardiziranih, preverjenih rešitev ter metodologij in sledenje predpisanim standardom.

Literatura

[1] (2015) Zakon o plačilnih storitvah in sistemih (ZPlaSS) . Dostopno na: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5485

[2] (2011) ZELENA KNJIGA Na poti k integriranemu evropskemu trgu za kartična, spletna in mobilna plačila. Dostopno na: http://eur-lex.europa.eu/legal-content/sl/TXT/?uri=CELEX%3A52011DC0941

[3] Banka Slovenije, Plačilni instrumenti. Dostopno na: https://www.bsi.si/placilni-sistemi.asp?MapaId=1431

[4] (23.11.2012) Krisper Boštjan ZPS, Posojilne kartice. Dostopno na: https://www.zps.si/index.php/osebne-finance-sp-1406526635/osebni-rauni/5910-posojilne-kartice

[5] (2013) Techno Buzz. Dostopno na: http://daniel-joel.blogspot.si/2013/12/smart-card-explained.html

[6] (27.11.2008) Emir Ugljanin, Milan Vidakovic i Goran Sladic. Autentifikacija platnih smart kartica . Dostopno na: http://2008.telfor.rs/files/radovi/09_26.pdf

[7] (20.01.1997) Aleksandar Jurišić, Alenka Trojar: Pametna kartica (Smart Card). Dostopno na: http://lkrv.fri.uni-lj.si/popularizacija/pametne_kartice97.pdf

[8] Uradni list RS.90/2006 Navodilo za izvajanje Sklepa o pošiljanju podatkov o uporabi sodobnih plačilnih instrumentov, Stran 9716.

[9] (2015) Stran Združenje bank Slovenije. Dostopno na: ZBS_PCI_DSS_Smernice_za_Trgovce_marec_2015

[10] (2016) Stran PCI SSC. Dostopno na: https://www.pcisecuritystandards.org/

[11] (2016) Stran PCI SSC**.** Dostopno na: https://www.pcisecuritystandards.org/pci_security/glossary

[12] (23.05.2011) Gorazd Žagar, Informacijska Varnost, PCI DSS v2. Dostopno na: http://infosec.si/?p=284

[13] (23.06.2012) Peter Brenko, Za tiste, ki se prvič podajate v spletno prodajo. Dostopno na: http://www.shopamine.com/za-tiste-ki-se-prvic-podajate-spletno-prodajo/

[14] (2010) Fakultete za Računalništvo in informatiko, Laboratorij za informatiko. Metodologija strateškega planiranja informatike s pristopom poslovno-informacijske arhitekture. Metodologija SPI in PIA.pdf

[15] Center za varnejši internet, Slovar pojmov. Mobilna naprava. Dostopno na: http://safe.si/pojmi/mobilna-naprava

[16] (2015) Smart Card Alliance, NFC Frequently Asked Questions. Dostopno na: http://www.smartcardalliance.org/downloads/NFC-Facts-at-a-Glance-Final-123115.pdf

[17] BSE Consulting, Methodology . Dostopno na: http://www.bse-c.co.kr/en/company/methodology

[18] ELEKTROTEHNIŠKO-RAČUNALNIŠKA STRO**K**OVNA ŠOLA IN GIMNAZIJA LJUBLJANA, SKRBNIK INFORMACIJSKIH SISTEMOV. Dostopno na: http://www.vegova.si/S5320/Skrbnik+informacijskih+sistemov-Skrbnik+komunikacijskih+sistemov

[19] ECB, Statistical Data Warehouse. Dostopno na: https://www.ecb.europa.eu/press/pr/date/2014/html/pr140429.sl.html

[20] Ovum TMT intelligence. Dostopno na: http://www.ovum.com/press_releases/global-mobile-proximity-payment-users-to-surpass-1-billion-by-2019/

[21] What's in the Magnetic Stripe. Dostopno na: http://www.plasticrewards.com/blog/whats-in-the-magnetic-stripe/

[22] SMART CARD-EXPLAINED. Dostopno na: http://daniel-joel.blogspot.si/2013/12/smart-card-explained.html

[23] Credit Card processing Guide. Dostopno na: https://www.cardfellow.com/credit-card-processing-guide/

[24] Information on Credit Card Interchange. Dostopno na: http://www.electronictransfer.com/blog/merchant-account-questions/information-on-credit-card-interchange